DrayTek

Vigor2820 Series

ADSL2/2+ Security Firewall

Your reliable networking solutions partner

User's Guide

V3.0

Vigor2820 Series
ADSL2/2+ Security Firewall
User's Guide

Version: 3.0

Date: 30/07/2009

Copyright Information

Copyright Declarations

Copyright 2009 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor router via http://www.draytek.com.

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: Vigor2820 Series Router

DrayTek Corp. declares that Vigor2820 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class B and EN55024/Class B.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN60950-1.

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device may accept any interference received, including interference that may cause undesired operation.

.

http://www.draytek.com/user/AboutRegulatory.php

Table of Contents

1 Preface 1

1.1 Web Configuration Buttons Explanation 1

1.2 LED Indicators and Connectors 2

1.2.1 For Vigor2820 3
1.2.2 For Vigor2820n 5
1.2.3 For Vigor2820V 7
1.2.4 For Vigor2820Vn 9
1.2.5 For Vigor2820VS 11
1.2.6 For Vigor2820VSn 13

1.3 Hardware Installation 15

1.4 ISDN Phone Adapter Installation 16

1.5 Printer Installation 17

2 Configuring Basic Settings 23

2.1 Changing Password 23

2.2 Quick Start Wizard 25

2.2.1 PPPoE/PPPoA 26
2.2.2 1483 Bridged IP 28
2.2.3 1483 Routed IP 29

2.3 Online Status 30

2.4 Saving Configuration 33

3 Advanced Web Configuration 35

3.1 WAN 35

3.1.1 Basics of Internet Protocol (IP) Network 35
3.1.2 Network Connection by 3G USB Modem 36
3.1.3 General Setup 36
3.1.4 Internet Access 39
3.1.5 Multi-PVCs 53
3.1.6 Load-Balance Policy 57

3.2 LAN 59

3.2.1 Basics of LAN 59
3.2.2 General Setup 61
3.2.3 Static Route 63
3.2.4 VLAN 66
3.2.5 Bind IP to MAC 67

3.3 NAT 68

3.3.1 Port Redirection 69
3.3.2 DMZ Host 71

3.3.3 Open Ports 74
3.4 Firewall 76
3.4.1 Basics for Firewall 76
3.4.2 General Setup 78
3.4.3 Filter Setup 80
3.4.4 DoS Defense 86
3.5 Objects Setting 89
3.5.1 IP Object 89
3.5.2 IP Group 91
3.5.3 Service Type Object 92
3.5.4 Service Type Group 94
3.5.5 Keyword Object 95
3.5.6 Keyword Group 96
3.5.7 File Extension Object 97
3.5.8 IM Object 98
3.5.9 P2P Object 100
3.5.10 Protocol Object 101
3.5.11 Misc Object 102
3.6 CSM 103
3.6.1 IM/P2P Filter Profile 105
3.6.2 URL Content Filter 106
3.6.3 Web Content Filter 110
3.7 Bandwidth Management 112
3.7.1 Sessions Limit 112
3.7.2 Bandwidth Limit 113
3.7.3 Quality of Service 115
3.8 Applications 121
3.8.1 Dynamic DNS 121
3.8.2 Schedule 123
3.8.3 RADIUS 125
3.8.4 UPnP 126
3.8.5 IGMP 128
3.8.6 Wake on LAN 129
3.9 VPN and Remote Access 130
3.9.1 Remote Access Control 130
3.9.2 PPP General Setup 131
3.9.3 IPSec General Setup 132
3.9.4 IPSec Peer Identity 133
3.9.5 Remote Dial-in User 135
3.9.6 LAN to LAN 138
3.9.7 Connection Management 146
3.10 Certificate Management 147
3.10.1 Local Certificate 147
3.10.2 Trusted CA Certificate 149
3.10.3 Certificate Backup 150
3.11 VoIP 150
3.11.1 DialPlan 152
3.11.2 SIP Accounts 161
3.11.3 Phone Settings 165
3.11.4 Status 182
3.12 ISDN 183

3.12.1 Basic Concept 183
3.12.2 General Settings 184
3.12.3 Dial to Single/Dual ISPs 187
3.12.4 Call Control 191

3.13 Wireless LAN 192

3.13.1 Basic Concepts 192
3.13.2 General Setup 194
3.13.3 Security 197
3.13.4 Access Control 198
3.13.5 WPS 200
3.13.6 WDS 202
3.13.7 Advanced Setting 205
3.13.8 WMM Configuration 206
3.13.9 AP Discovery 207
3.13.10 Station List 208

3.14 USB Application 209

3.14.1 USB General Settings 209
3.14.2 FTP User Management 210
3.14.3 Disk Status 211

3.15 System Maintenance 212

3.15.1 System Status 212
3.15.2 TR-069 214
3.15.3 Administrator Password 215
3.15.4 Configuration Backup 215
3.15.5 Syslog/Mail Alert 217
3.15.6 Time and Date 218
3.15.7 Management 220
3.15.8 Reboot System 221
3.15.9 Firmware Upgrade 222

3.16 Diagnostics 223

3.16.1 Dial-out Trigger 223
3.16.2 Routing Table 224
3.16.3 ARP Cache Table 224
3.16.4 DHCP Table 225
3.16.5 NAT Sessions Table 225
3.16.6 Ping Diagnosis 226
3.16.7 Data Flow Monitor 227
3.16.8 Traffic Graph 228
3.16.9 Trace Route 229

Application and Examples 231

4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter 231

4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter 238

4.3 QoS Setting Example 243

4.4 LAN – Created by Using NAT 246

4.5 Calling Scenario for VoIP function 248

4.5.1 Calling via SIP Sever 248
4.5.2 Peer-to-Peer Calling 250

4.6 Upgrade Firmware for Your Router 251

4.7 Request a certificate from a CA server on Windows CA Server 253
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server 257

Trouble Shooting 259

5.1 Checking If the Hardware Status Is OK or Not..... 259
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not 260
5.3 Pinging the Router from Your Computer 262
5.4 Checking If the ISP Settings are OK or Not..... 263
5.5 Problems for 3G Network Connection 265
5.6 Backing to Factory Default Setting If Necessary 266
5.7 Contacting Your Dealer 267

Appendix: Hardware Specifications.....269

1 Preface

Vigor2820 series is an ADSL and broadband router with WAN interface. It provides policy-based load-balance, fail-over and BOD (Bandwidth on Demand), also it integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DS, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 32 VPN tunnels.

The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger) and P2P (Peer to Peer) more efficiency than before. By the way, DoS/DDoS prevention and URL/Web content filter strengthen the security outside and control inside.

Vigor2820 "S" series models support two ISDN ports. Phone S0 port is dedicated for ISDN phone and ISDN/Phone S0 port is configurable for ISDN line and phone if required. It can support multiple SIP registrars with high flexible configuration and call handling options.

Object-based firewall is flexible and allows your network be safe. In addition, through VoIP function, the communication fee for you and remote people can be reduced.

1.1 Web Configuration Buttons Explanation

Several main buttons appeared on the web pages are defined as the following:

OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified item.
Edit	Edit the settings for the selected item.
Delete	Delete the selected item with the corresponding settings.

Note: For the other buttons shown on the web pages, please refer to Chapter 4 for detailed explanation.

1.2 LED Indicators and Connectors

Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.

The displays of LED indicators and connectors for the routers are different slightly. The following sections will introduce them respectively. If the model of router you have does not support ISDN and/or VoIP function, simply ignore the relational description.

Definitions for ISDN Ports

Below shows the names that displayed on front panel of the device and the WEB UI of this device.

ISDN TE (Terminal Equipment) means an interface for transmitting analog signal through Internet between Switching and router. Such interface is also named with **ISDN S0 extern** in Germany.

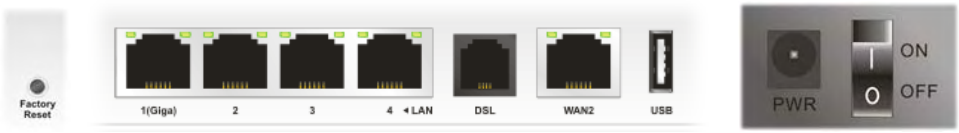
ISDN NT (Network Terminator) is a port that used to connect general phone. Such interface is also named with **ISDN S0 intern** in Germany.

The **Phone S0** port is fixed to connect phone forever and the LED on the connecter will light orange always. However **ISDN/Phone S0** port on this device is configurable for connecting phone or accessing Internet according to the settings that you adjust on WEB UI (please refer to **VoIP>>Phone Setting** for detailed information).

Warning: When the orange LED lights (means ISDN NT mode), the ISDN port can be used to connect phone only. Wrong ISDN connection might cause severe damage on your device.

1.2.1 For Vigor2820

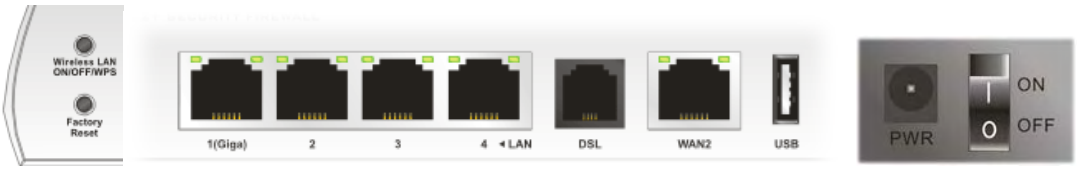
LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is enabled from **Firewall >> General Setup**. (Such profile is established under **CSM** menu).
WCF		On	The Web Content Filter is active. (It is enabled from **Firewall >> General Setup** and the web content filter profile is established under **CSM** menu.)
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The DSL connection is ready. Quickly: The connection is tranning.
WAN2		On	The router is ready to access Internet through WAN connection.
		Blinking	It will blink while transmitting data.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while deleting an attack.
VPN		On	The VPN tunnel is active.
QoS		On	The QoS function is active.
LED on Connector			
LAN 1(Giga)	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected with 10/100Mbps.
LAN 2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.
WAN 2	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.



Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
LAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN 2	Connecter for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

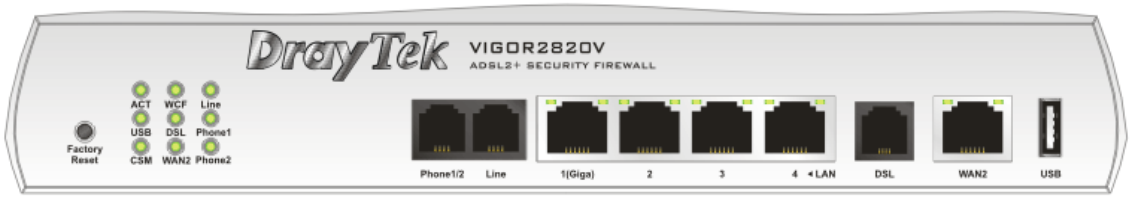
1.2.2 For Vigor2820n

LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is enabled from **Firewall >> General Setup**. (Such profile is established under **CSM** menu).
WLAN		On	Wireless access point is ready.
		Blinking	It will blink while wireless traffic goes through.
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The DSL connection is ready. Quickly: The connection is training.
WAN2		On	The router is ready to access Internet through WAN connection.
		Blinking	It will blink while transmitting data.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while deleting an attack.
VPN		On	The VPN tunnel is active.
QoS		On	The QoS function is active.
LED on Connector			
LAN 1(Giga)	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected with 10/100Mbps.
LAN 2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.
WAN 2	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.

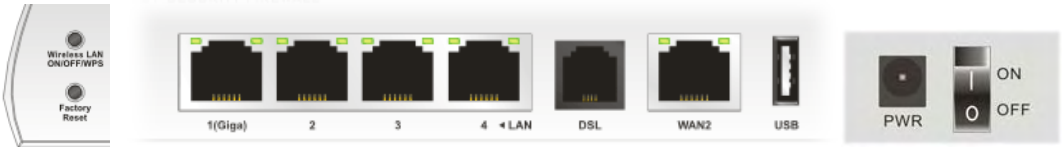


Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button for 2 seconds to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
LAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN 2	Connecter for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.3 For Vigor2820V

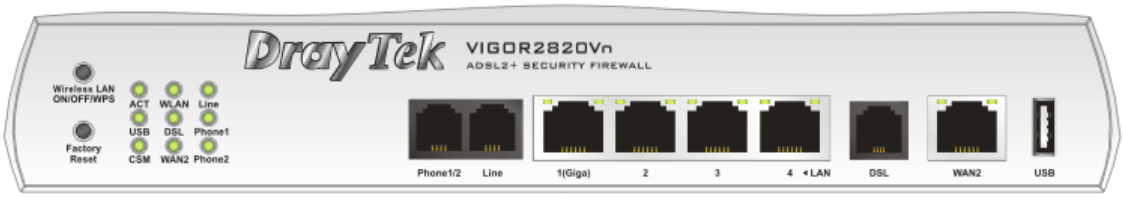


LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is enabled from **Firewall** >> **General Setup**. (Such profile is established under **CSM** menu).
WCF		On	The Web Content Filter is active. (It is enabled from **Firewall** >> **General Setup** and the web content filter profile is established under **CSM** menu.)
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The modem is ready. Quickly: The connection is training.
WAN2		On	The router is ready to access Internet through WAN connection.
		Blinking	It will blink while transmitting data.
Line		On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off about six seconds later.
		Off	There is no PSTN phone call.
Phone 1/2		On	The phone connected to this port is off-hook.
		Off	The phone connected to this port is on-hook.
LED on Connector			
LAN 1(Giga)	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is connected with 10/100Mbps.
LAN 2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is connected with 10Mbps.
WAN 2	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is connected with 10Mbps.

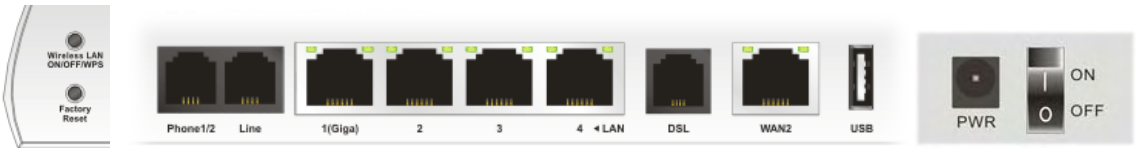


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
LAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN 2	Connecter for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.4 For Vigor2820Vn

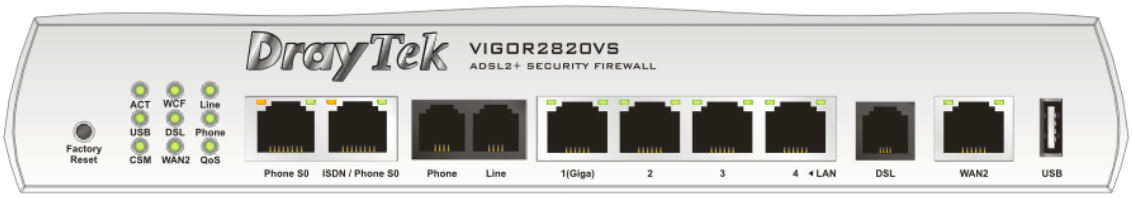


LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is enabled from **Firewall >> General Setup**. (Such profile is established under **CSM** menu).
WLAN		On	Wireless access point is ready.
		Blinking	It will blink while wireless traffic goes through.
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The DSL connection is ready. Quickly: The connection is tranning.
WAN 2	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.
Line		On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off about six seconds later.
		Off	There is no PSTN phone call.
Phone 1/2		On	The phone connected to this port is off-hook.
		Off	The phone connected to this port is on-hook.
		Blinking	A phone call comes.
LED on Connector			
LAN 1(Giga)	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected with 10/100Mbps.
LAN 2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.
WAN 2	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.



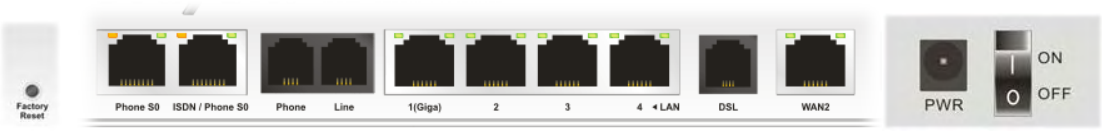
Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button for 2 seconds to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
Phone 1/2	Connecter for PSTN phone.
Line	Connector for PSTN life line.
LAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN 2	Connecter for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.5 For Vigor2820VS



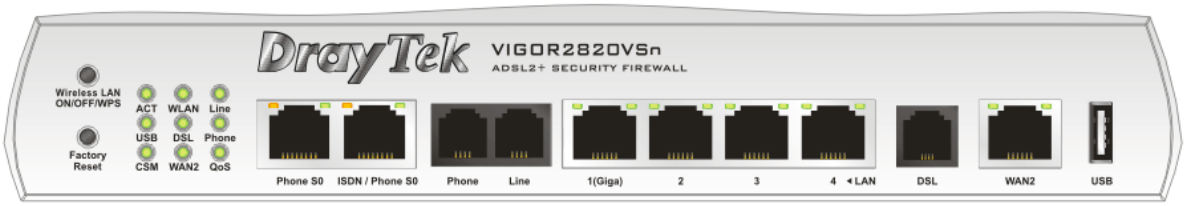
LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is enabled from **Firewall** >> **General Setup**. (Such profile is established under **CSM** menu).
WCF		On	The Web Content Filter is active. (It is enabled from **Firewall** >> **General Setup** and the web content filter profile is established under **CSM** menu.)
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The DSL connection is ready. Quickly: The connection is tranning.
WAN 2		On	The WAN1 or WAN2 connection is ready.
		Blinking	It will blink while transmitting data.
Line		On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off about six seconds later.
		Off	There is no PSTN phone call.
Phone		On	The phone connected to this port is off-hook.
		Off	The phone connected to this port is on-hook.
		Blinking	A phone call comes.
QoS		On	The QoS function is active.
LED on Connector			
Phone S0	Left LED (Orange)	On	ISDN NT (ISDN S0 intern) mode is active and an ISDN phone adapter is connected.
		Blinking	ISDN NT (ISDN S0 intern) mode is active and an ISDN phone adapter is not connected.
	Right LED (Green)	On	A phone has been connected. If not, green LED will be off.
		Blinking	An ISDN phone is off-hook or a phone call comes.
ISDN/ Phone S0	Left LED (Orange)	On	ISDN NT (ISDN S0 intern) mode is active configured from **VoIP**>>**Phone Settings** and an ISDN phone adapter is connected.
		Blinking	ISDN NT (ISDN S0 intern) mode configured from **VoIP**>>**Phone Settings** is active and an ISDN phone adapter is not connected.
		Off	It means ISDN TE mode is active which is configured from **VoIP**>>**Phone Settings**.
	Right LED (Green)	On	A phone adapter with phone set has been connected (ISDN S0 intern mode) or ISDN line has been connected (ISDN S0 extern mode). It will be off if there is nothing connected.
		Blinking	In ISDN NT (ISDN S0 intern) mode, it means an ISDN phone is off-hook or a phone call comes. In ISDN TE mode, it means data, fax or voice (phone call) is transmitting.

LAN 1(Giga)	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected with 10/100Mbps.
LAN 2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.
WAN 2	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.



Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
Phone S0	Connecter for ISDN phone(s) only via ISDN phone adapter. Do not connect any other device to such port or connect ISDN line, otherwise the router might be damaged.
ISDN/Phone S0	Connecter for ISDN line or ISDN phone adapter in particular condition. Refer to section 2.2 for more details.
Phone	Connecter for PSTN phone.
Line	Connector for PSTN life line.
LAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN 2	Connecter for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.6 For Vigor2820VSn



LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is enabled from **Firewall >> General Setup**. (Such profile is established under **CSM** menu).
WLAN		On	Wireless access point is ready.
		Blinking	It will blink while wireless traffic goes through.
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The DSL connection is ready. Quickly: The connection is training.
WAN 2		On	The WAN1 or WAN2 connection is ready.
		Blinking	It will blink while transmitting data.
Line		On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off about six seconds later.
		Off	There is no PSTN phone call.
Phone		On	The phone connected to this port is off-hook.
		Off	The phone connected to this port is on-hook.
		Blinking	A phone call comes.
QoS		On	The QoS function is active.
LED on Connector			
Phone S0	Left LED (Orange)	On	ISDN NT (ISDN S0 intern) mode is active and an ISDN phone adapter is connected.
		Blinking	ISDN NT (ISDN S0 intern) mode is active and an ISDN phone adapter is not connected.
	Right LED (Green)	On	A phone has been connected. If not, green LED will be off.
		Blinking	An ISDN phone is off-hook or a phone call comes.
ISDN/ Phone S0	Left LED (Orange)	On	ISDN NT (ISDN S0 intern) mode is active configured from **VoIP>>Phone Settings** and an ISDN phone adapter is connected.
		Blinking	ISDN NT (ISDN S0 intern) mode configured from **VoIP>>Phone Settings** is active and an ISDN phone adapter is not connected.
		Off	It means ISDN TE mode is active which is configured from **VoIP>>Phone Settings**.
	Right LED (Green)	On	A phone adapter with phone set has been connected (ISDN S0 intern mode) or ISDN line has been connected (ISDN S0 extern mode). It will be off if there is nothing connected.
		Blinking	In ISDN NT (ISDN S0 intern) mode, it means an ISDN phone is off-hook or a phone call comes. In ISDN TE mode, it means data, fax or voice (phone call) is transmitting.

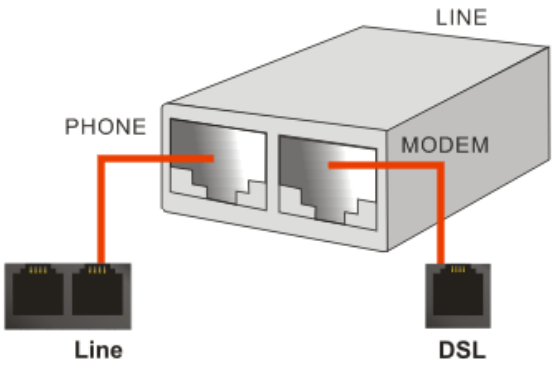
LAN 1(Giga)	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected with 10/100Mbps.
LAN 2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.
WAN 2	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is disconnected with 10Mbps.

Interface	Description
Wireless LAN ON/OFF/WPS	Press "Wireless LAN ON/OFF/WPS" button for 2 seconds to wait for client device making network connection through WPS. Press "Wireless LAN ON/OFF/WPS" button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
Phone S0	Connecter for ISDN phone(s) only via ISDN phone adapter. Do not connect any other device to such port or connect ISDN line, otherwise the router might be damaged.
ISDN/Phone S0	Connecter for ISDN line or ISDN phone adapter in particular condition. Refer to section 2.2 for more details.
Phone	Connecter for PSTN phone.
Line	Connector for PSTN life line.
LAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN 2	Connecter for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.3 Hardware Installation

Before starting to configure the router, you have to connect your devices correctly.

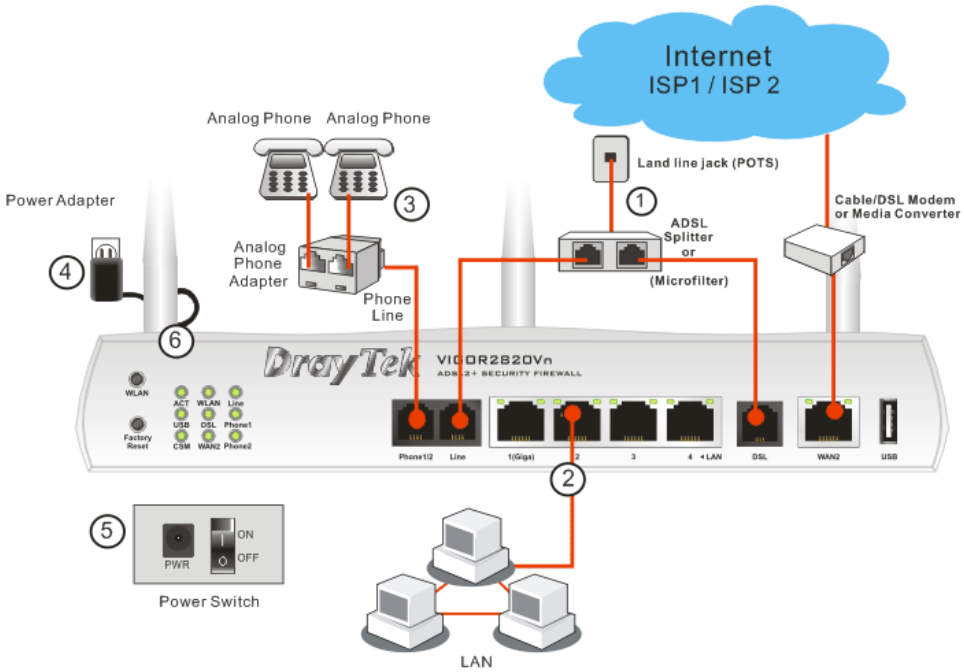
1. Connect the ADSL interface to the external ADSL splitter with an ADSL line cable for all models. For Vigor2820Vn/VS/VSn, also connect Line interface to external ADSL splitter.



   For second WAN, connect the cable Modem/DSL Modem/Media Converter to WAN2 port of router with Ethernet cable (RJ-45).

2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
3. Connect the telephone set with phone lines (for using VoIP function). For the model without phone ports, skip this step.
4. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
5. Power on the device by pressing down the power switch on the rear panel.
6. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.

(For the hardware connection, we take *"Vn"* model as an example.)

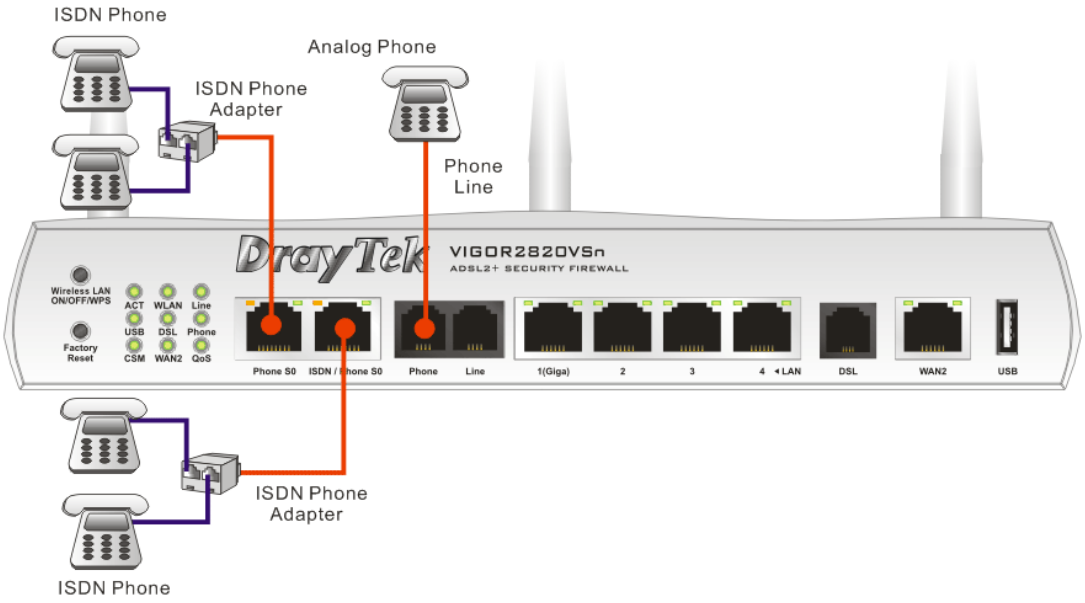


Caution: Each of the Phone ports can be connected to an analog phone only. Do not connect the phone ports to the telephone wall jack. Such connection might damage your router.

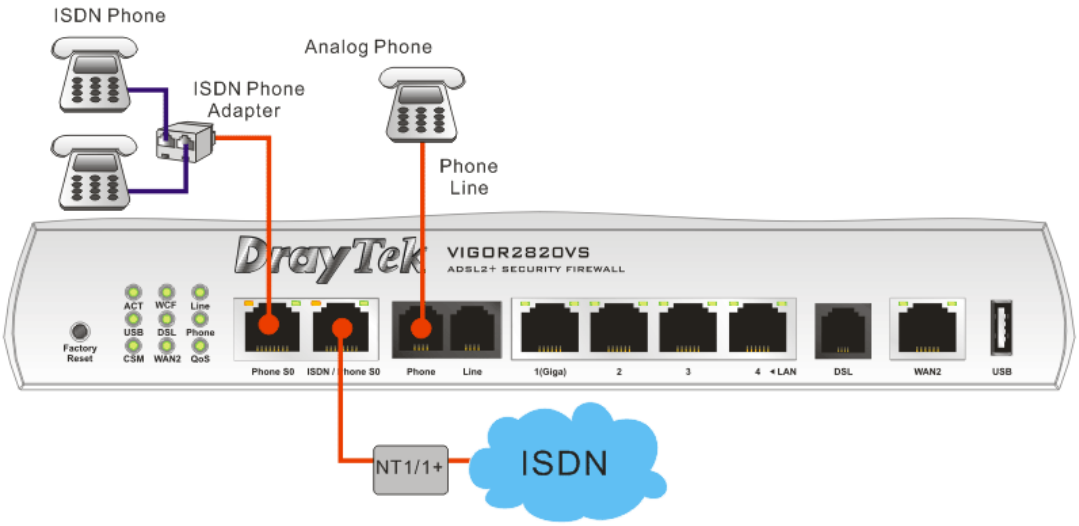
1.4 ISDN Phone Adapter Installation

Such information is provided for Vigor2820 S models (e.g., Vigor2820VS).

Phone S0 is always fixed to connect ISDN phone. However, ISDN /Phone S0 is configurable as NT or TE mode. When the user configures ISDN /Phone S0 as NT mode in **VoIP>> Phone Settings**, the **orange** LED will light on to indicate **ISDN-NT** is selected. And by using ISDN phone adapters (coming from the router package), the user can connect several phones to Vigor2820VS for communication. Refer to the following figure for reference.

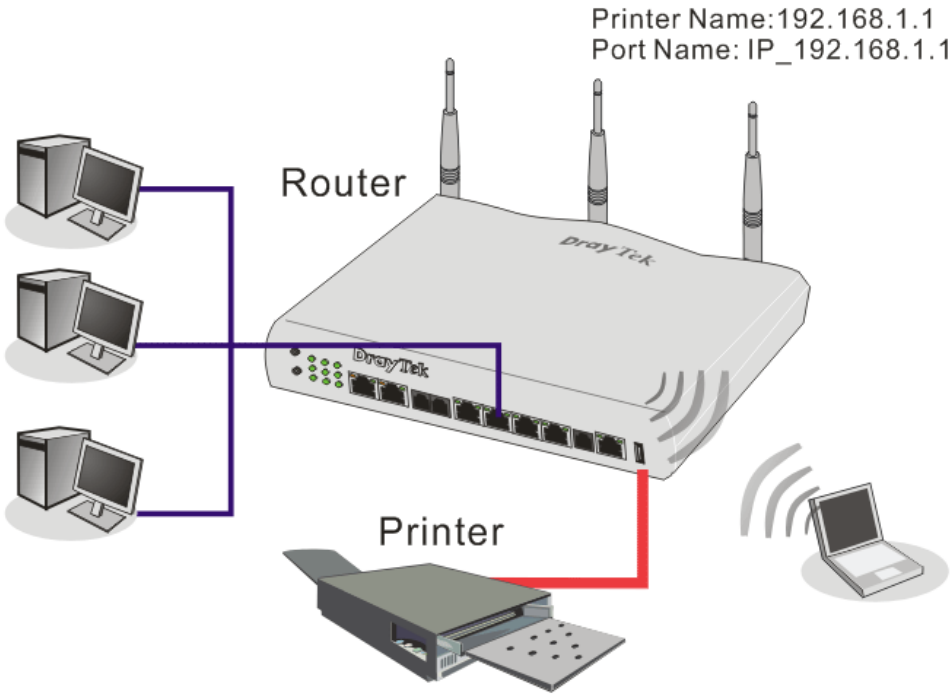


Yet, if the user configures ISDN / Phone S0 as TE Mode in **VoIP>> Phone Settings**, the **green** LED will light on to indicate **ISDN-TE** is selected. Then, the port is specified for ISDN line only. Refer to the following figure for reference.



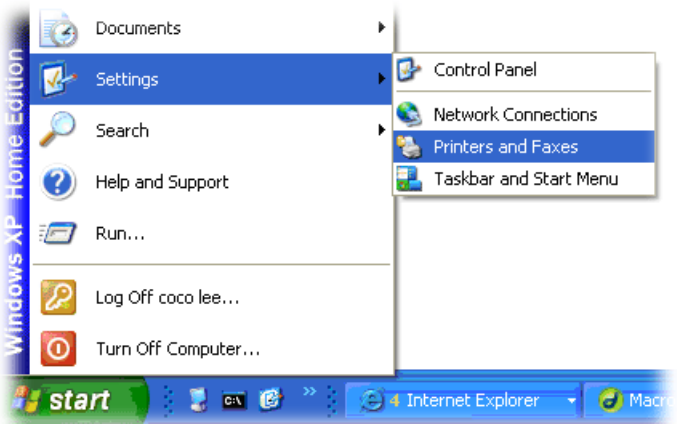
1.5 Printer Installation

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE, please visit www.draytek.com.

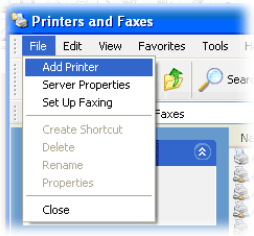


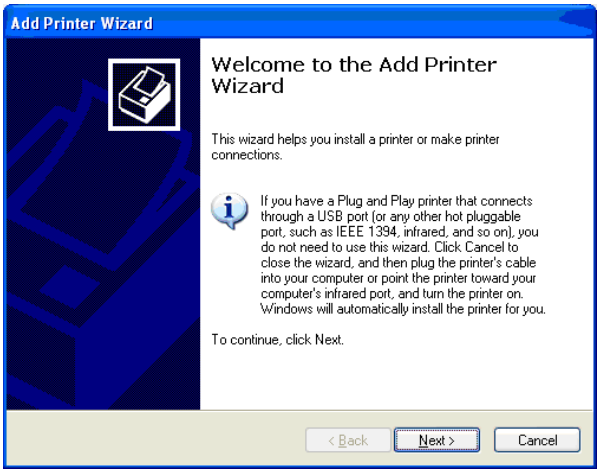
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

1. Connect the printer with the router through USB/parallel port.
2. Open **Start->Settings-> Printer and Faxes**.

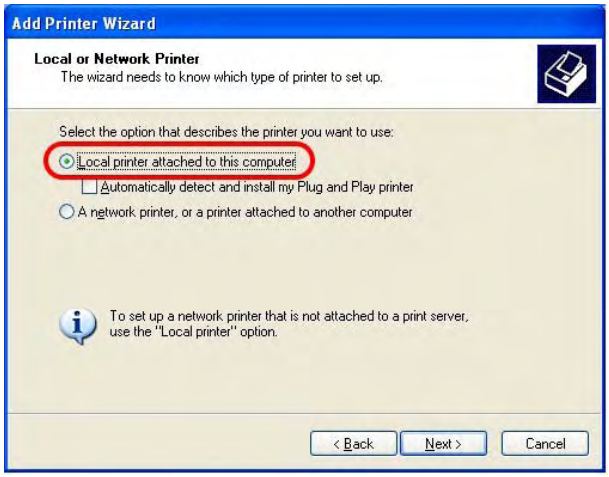


3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.




Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

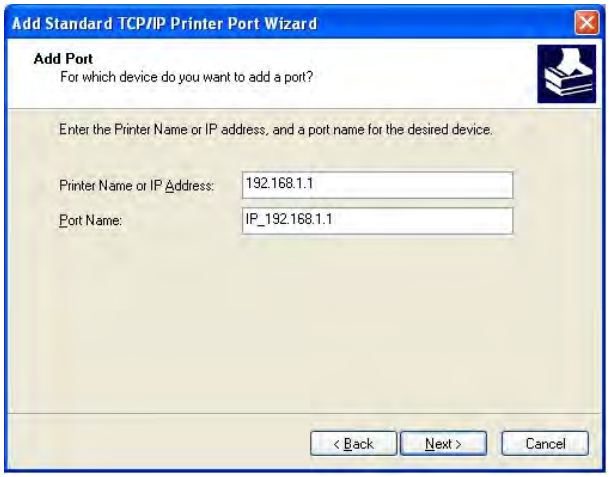
4. Click Local printer attached to this computer and click Next.


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.

Add Printer Wizard
Select a Printer Port
Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
Use the following port:
LPT1: (Recommended Printer Port)
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
Create a new port:
Type of port:
Standard TCP/IP Port
< Back
Next >
Cancel

6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name or IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.1.1
Port Name:
IP_192.168.1.1
< Back
Next >
Cancel

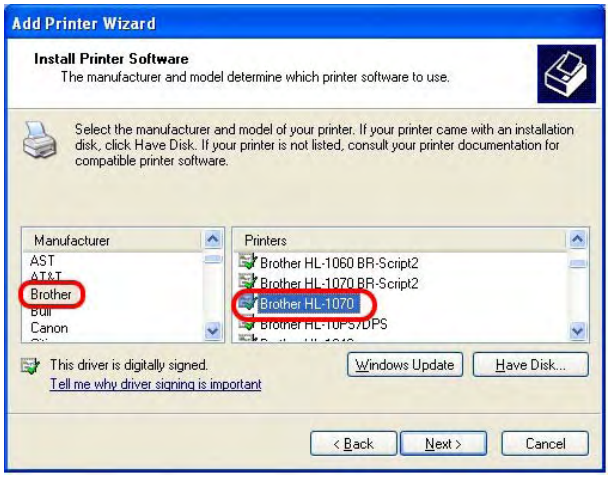
7. Click Standard and choose Generic Network Card.

Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The detected device is of unknown type. Be sure that:
1. The device is properly configured.
2. The address on the previous page is correct.
Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

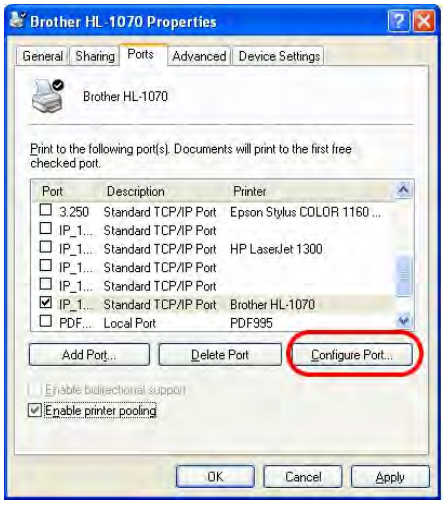
8. Then, in the following dialog, click **Finish**.

Add Standard TCP/IP Printer Port Wizard
Completing the Add Standard TCP/IP Printer Port Wizard
You have selected a port with the following characteristics.
SNMP: No
Protocol: RAW, Port 9100
Device: 192.168.1.1
Port Name: IP_192.168.1.1
Adapter Type: Generic Network Card
To complete this wizard, click Finish.
< Back
Finish
Cancel

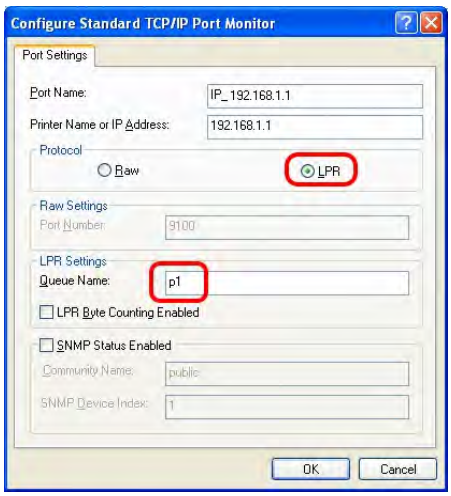
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.


Add Printer Wizard
Install Printer Software
The manufacturer and model determine which printer software to use.
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.
Manufacturer
AST
AT&T
Brother
Bull
Canon
Printers
Brother HL-1060 BR-Script2
Brother HL-1070 BR-Script2
Brother HL-1070
This driver is digitally signed.
Tell me why driver signing is important
Windows Update
Have Disk...
< Back
Next >
Cancel

10. For the final stage, you need to go back to **Control Panel-> Printers** and edit the property of the new printer you have added.

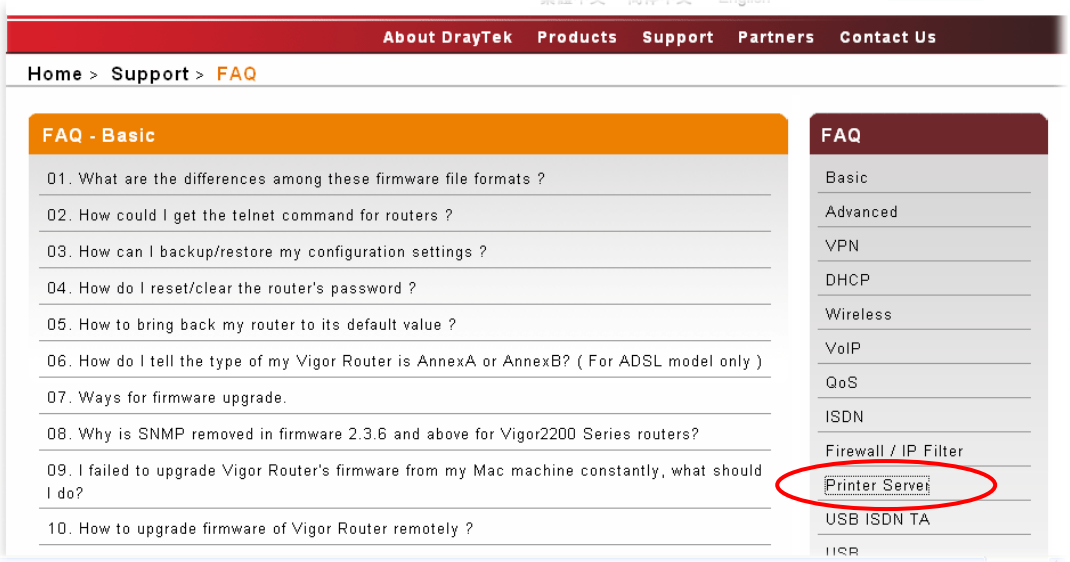


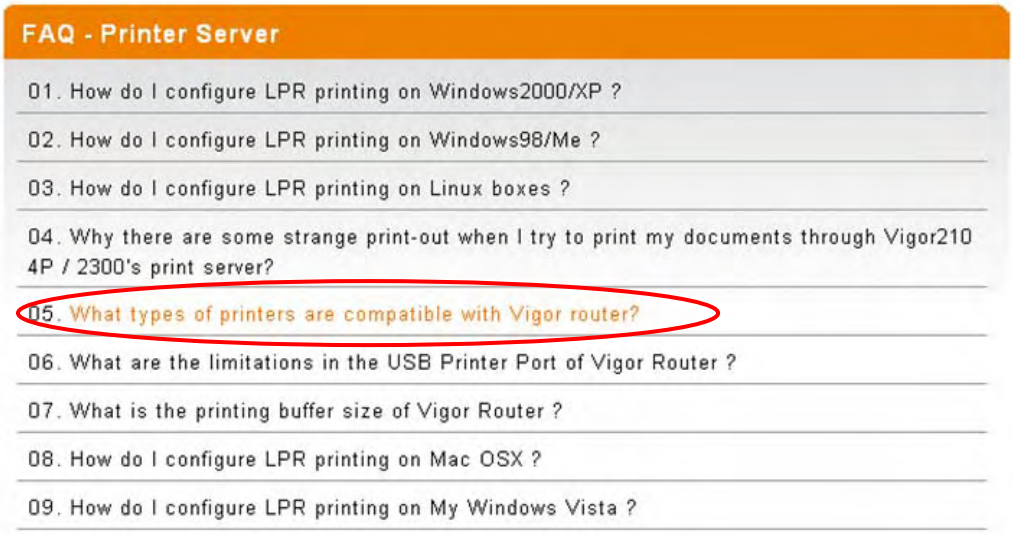
11. Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and UPR name.



The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support >FAQ**; find out the link of **Printer Server** and click it; then click the **What types of printers are compatible with Vigor router?** link.


About DrayTek
Products
Support
Partners
Contact Us
Home > Support > FAQ
FAQ - Basic
01. What are the differences among these firmware file formats ?
02. How could I get the telnet command for routers ?
03. How can I backup/restore my configuration settings ?
04. How do I reset/clear the router's password ?
05. How to bring back my router to its default value ?
06. How do I tell the type of my Vigor Router is AnnexA or AnnexB? (For ADSL model only)
07. Ways for firmware upgrade.
08. Why is SNMP removed in firmware 2.3.6 and above for Vigor2200 Series routers?
09. I failed to upgrade Vigor Router's firmware from my Mac machine constantly, what should I do?
10. How to upgrade firmware of Vigor Router remotely ?
FAQ
Basic
Advanced
VPN
DHCP
Wireless
VoIP
QoS
ISDN
Firewall / IP Filter
Printer Server
USB ISDN TA


FAQ - Printer Server
01. How do I configure LPR printing on Windows2000/XP ?
02. How do I configure LPR printing on Windows98/Me ?
03. How do I configure LPR printing on Linux boxes ?
04. Why there are some strange print-out when I try to print my documents through Vigor2104P / 2300's print server?
05. What types of printers are compatible with Vigor router?
06. What are the limitations in the USB Printer Port of Vigor Router ?
07. What is the printing buffer size of Vigor Router ?
08. How do I configure LPR printing on Mac OSX ?
09. How do I configure LPR printing on My Windows Vista ?

Note 2: Vigor router supports printing request from computers via LAN ports but not WAN port.

This page is left blank.

2 Configuring Basic Settings

For use the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

This chapter explains how to setup a password for an administrator and how to adjust basic settings for accessing Internet successfully. Be aware that only the administrator can change the router configuration.

2.1 Changing Password

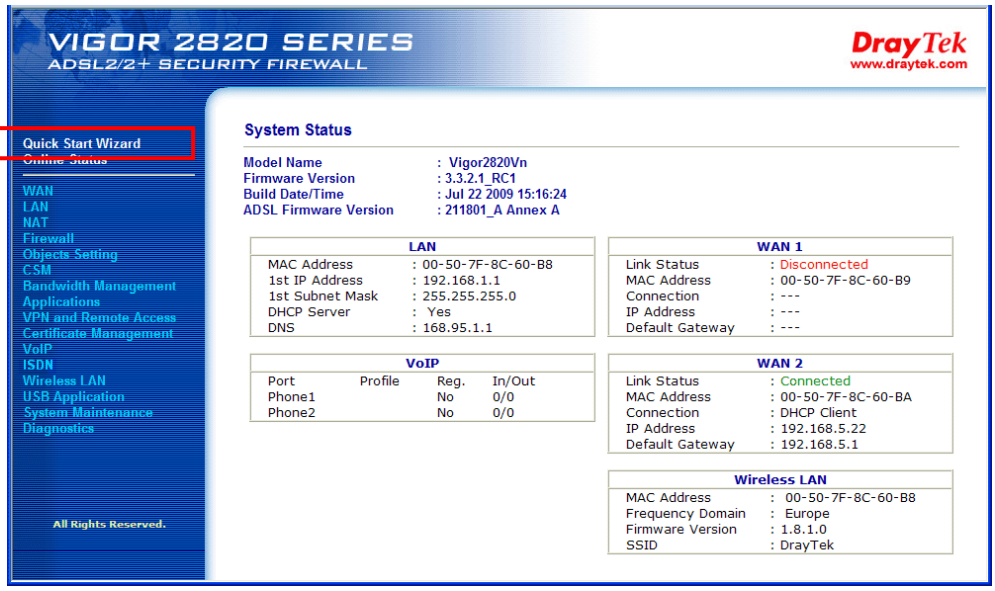
To change the password for this device, you have to access into the web browse with default password first.

1. Make sure your computer connects to the router correctly.

> **Notice:** You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of this guide.

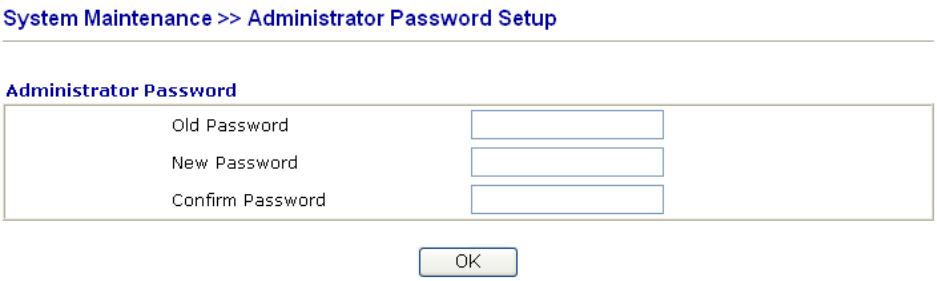
2. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Please type “admin” as the username and leave blank for the password on the window. Next click **OK** for next screen.

3. Now, the **Main Screen** will pop up.



Note: The home page will change slightly in accordance with the router you have.

4. Go to **System Maintenance** page and choose **Administrator Password**.

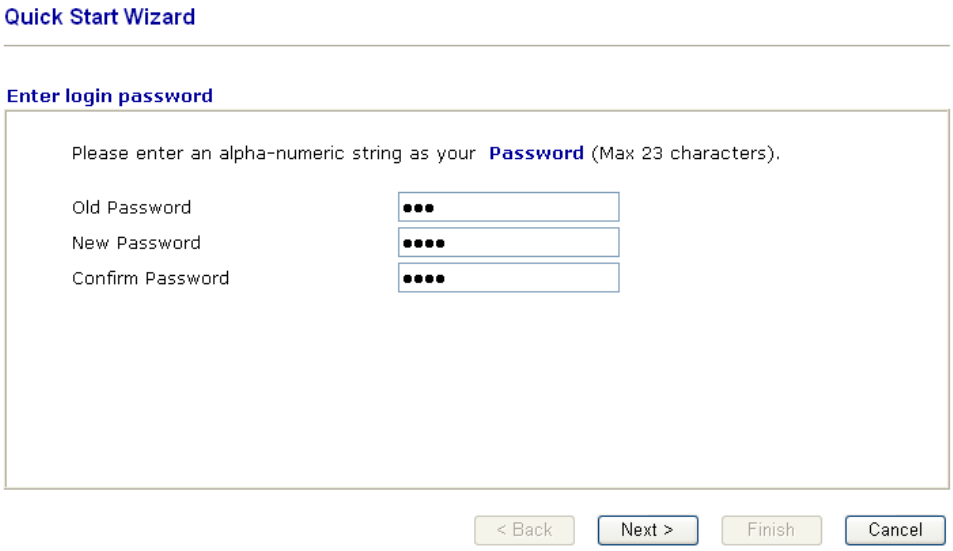


5. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.

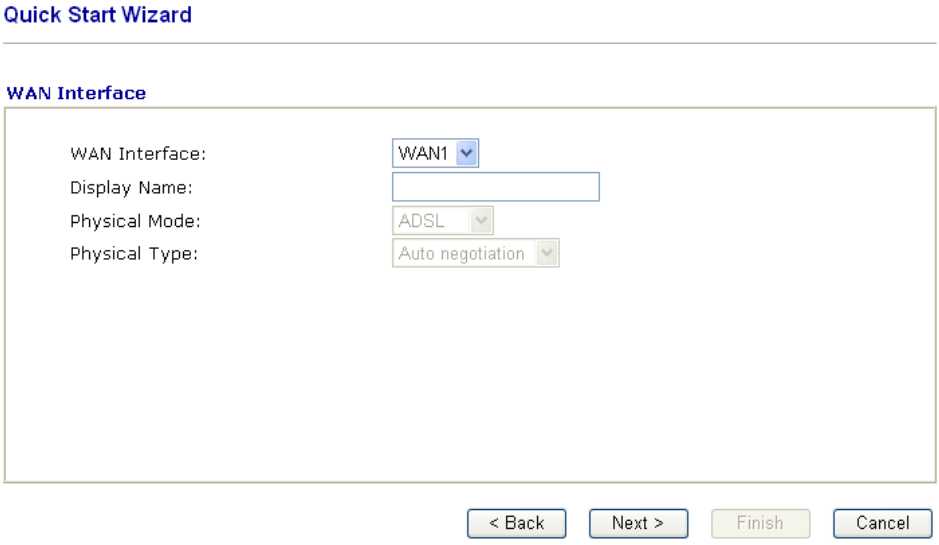
6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

2.2 Quick Start Wizard

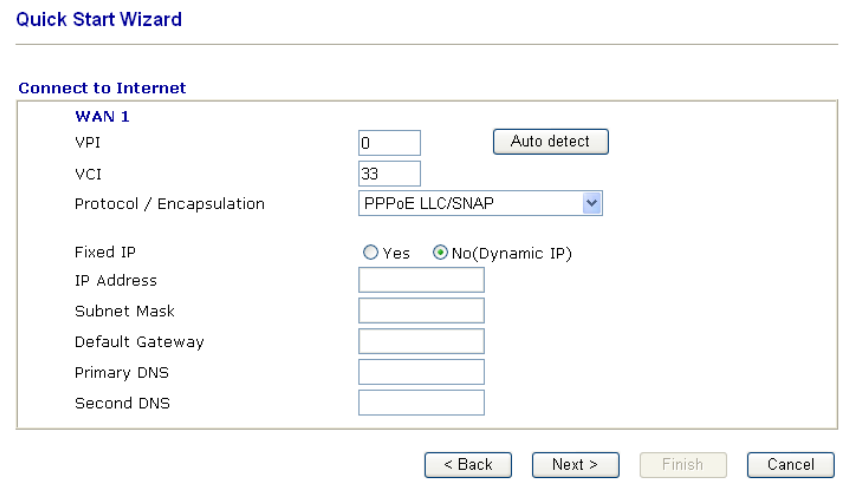
If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.

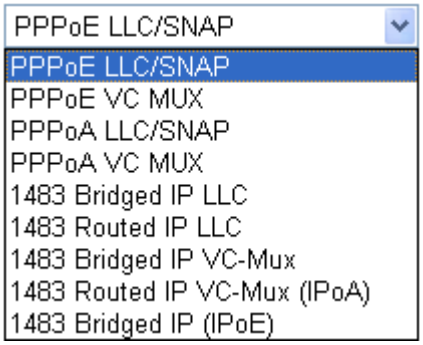


On the next page as shown below, please select the WAN interface (WAN 1 or WAN2) that you use. If DSL interface is used, please choose WAN1; if WAN2 interface is used, please choose WAN2. Choose **Auto negotiation** as the physical type for your router. Then click **Next** for next step.



On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.





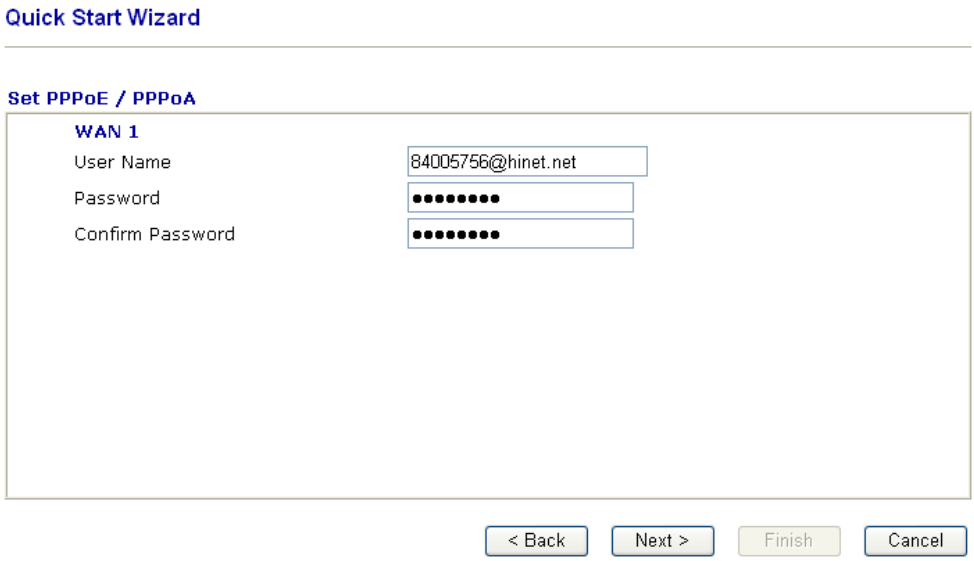
In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE/PPPoA**, **1483 Bridged IP** or **1483 Routed IP**. The router supports the DSL WAN interface for Internet access.

2.2.1 PPPoE/PPPoA

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

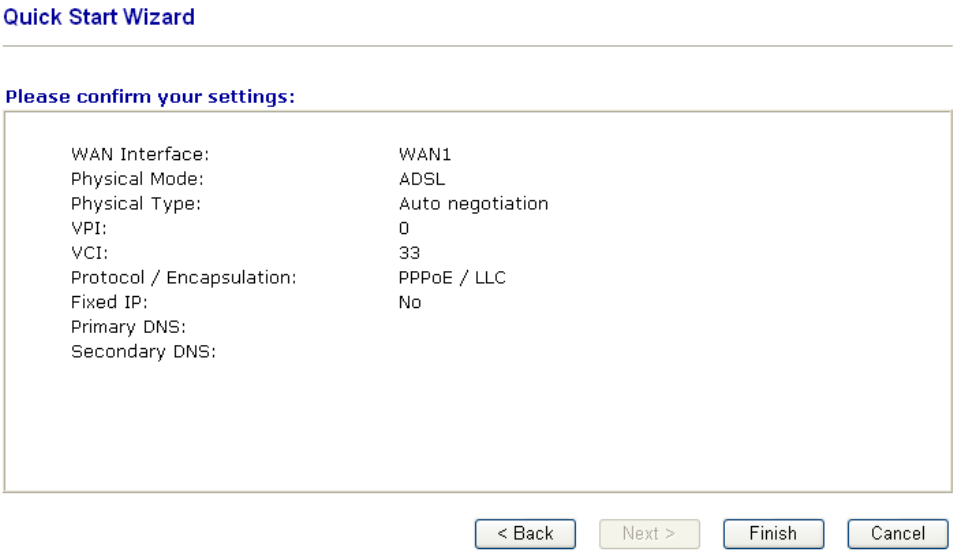
PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this router. The following page will be shown:



User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.

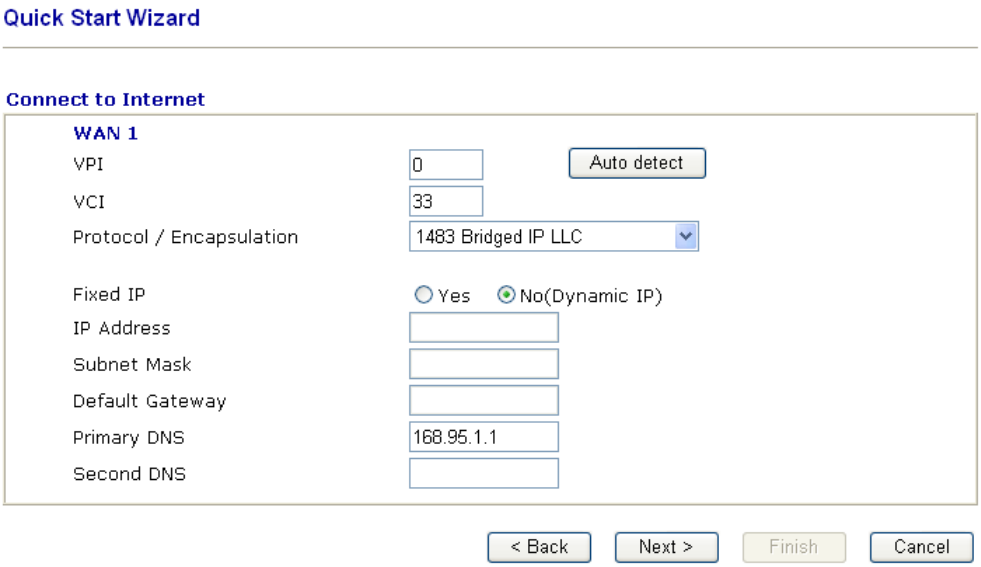
Click **Next** for viewing summary of such connection.



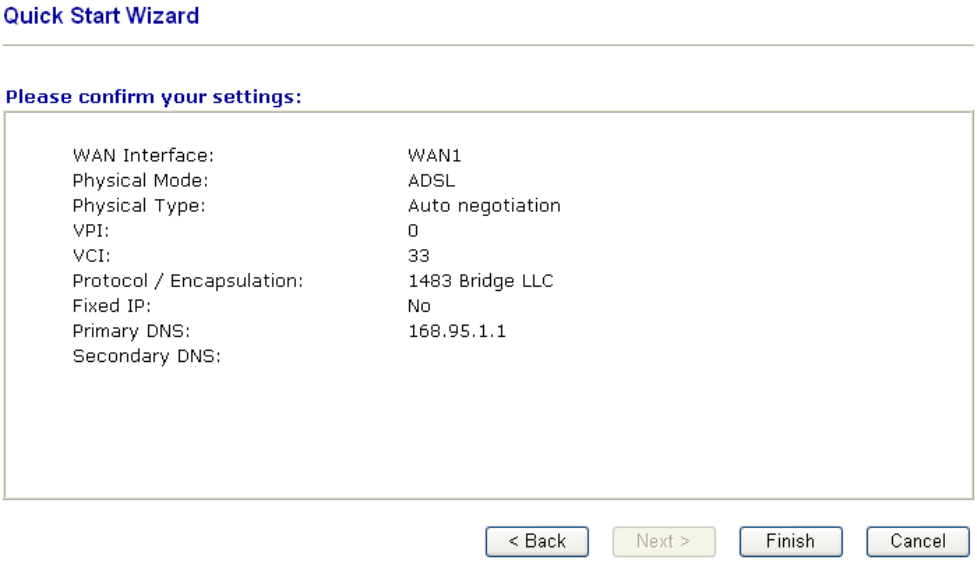
Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

2.2.2 1483 Bridged IP

Click **1483 Bridged IP** as the protocol. Type in all the information that your ISP provides for this protocol.



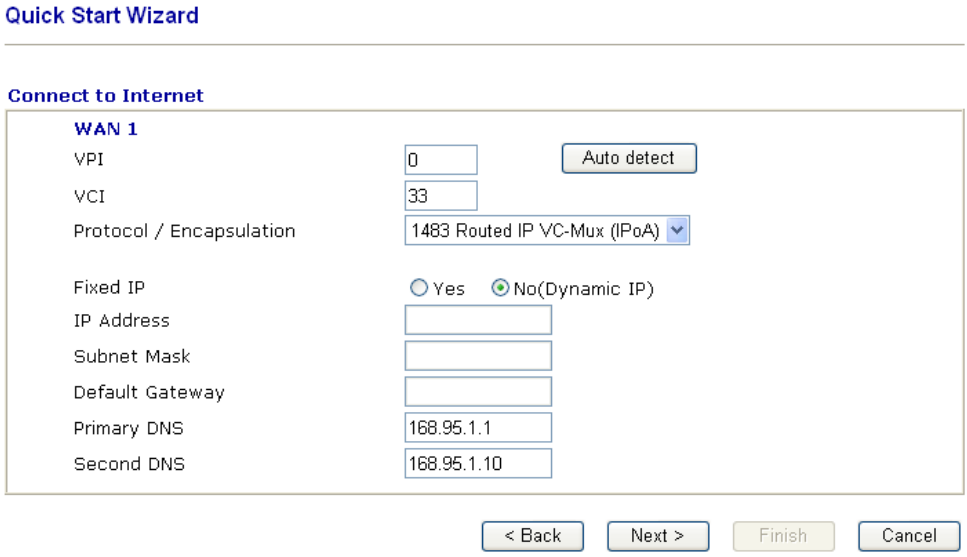
Click **Next** for viewing summary of such connection.



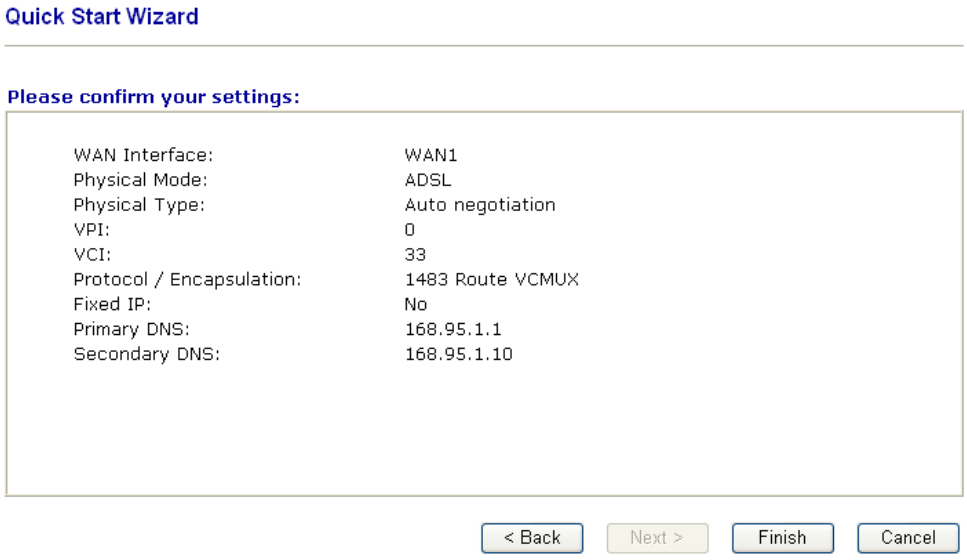
Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

2.2.3 1483 Routed IP

Click **1483 Routed IP** as the protocol. Type in all the information that your ISP provides for this protocol.



After finishing the settings in this page, click **Next** to see the following page.

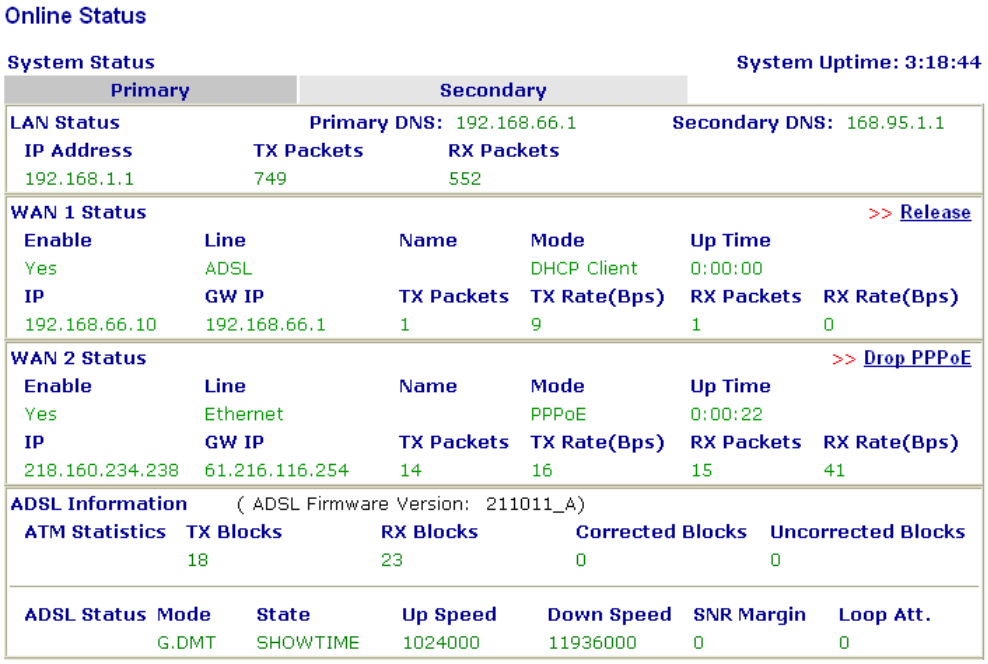


Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

2.3 Online Status

The online status shows the system status, WAN status, ADSL Information and other status related to this router within one page. If you select **PPPoE/PPPoA** as the protocol, you will find out a link of **Dial PPPoE** or **Drop PPPoE** in the Online Status web page.

Online status for PPPoE (WAN2)



Online Status

System Status — System Uptime: 3:18:44

Primary	Secondary

LAN Status — Primary DNS: 192.168.66.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	749	552

WAN 1 Status — >> Release

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		DHCP Client	0:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.66.10	192.168.66.1	1	9	1	0

WAN 2 Status — >> Drop PPPoE

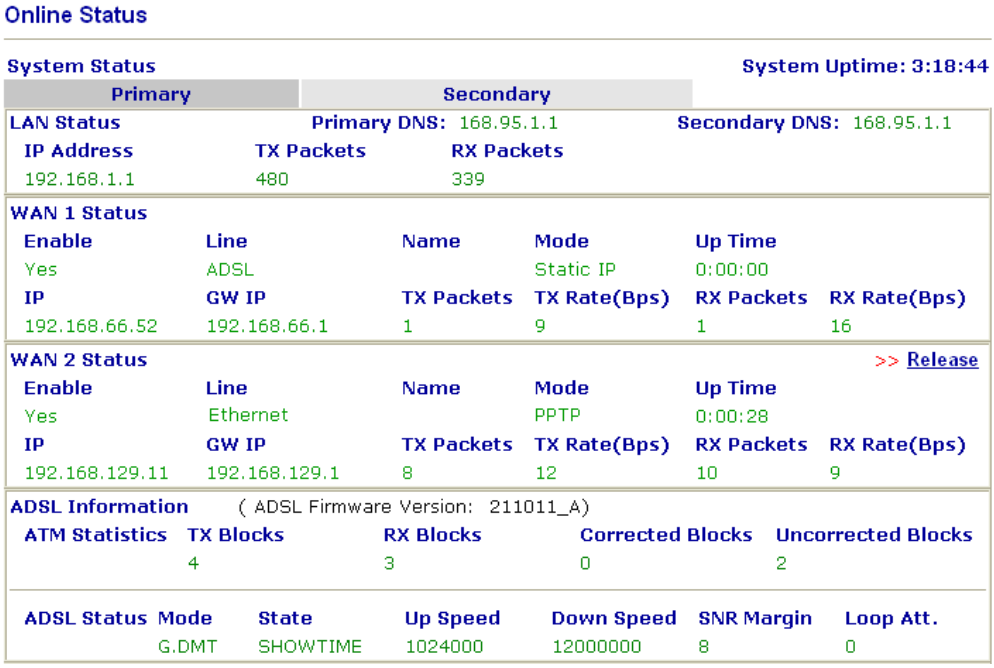
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:22	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
218.160.234.238	61.216.116.254	14	16	15	41

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	18	23	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	11936000	0	0

Online status for PPTP (for WAN2)



Online Status

System Status — System Uptime: 3:18:44

Primary	Secondary

LAN Status — Primary DNS: 168.95.1.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	480	339

WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.66.52	192.168.66.1	1	9	1	16

WAN 2 Status — >> Release

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPTP	0:00:28	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.129.11	192.168.129.1	8	12	10	9

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	4	3	0	2

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	12000000	8	0

Online status for Static IP (for WAN1)

Online Status

System Status — System Uptime: 3:18:44

Primary	Secondary

LAN Status — Primary DNS: 168.95.1.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	480	339

WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.52	192.168.66.1	1	9	1	16

WAN 2 Status — >> Release

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPTP	0:00:28	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.129.11	192.168.129.1	8	12	10	9

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	4	3	0	2

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	12000000	8	0

Online status for DHCP (WAN1)

Online Status

System Status — System Uptime: 3:18:44

Primary	Secondary

LAN Status — Primary DNS: 192.168.66.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	749	552

WAN 1 Status — >> Release

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		DHCP Client	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.10	192.168.66.1	1	9	1	0

WAN 2 Status — >> Drop PPPoE

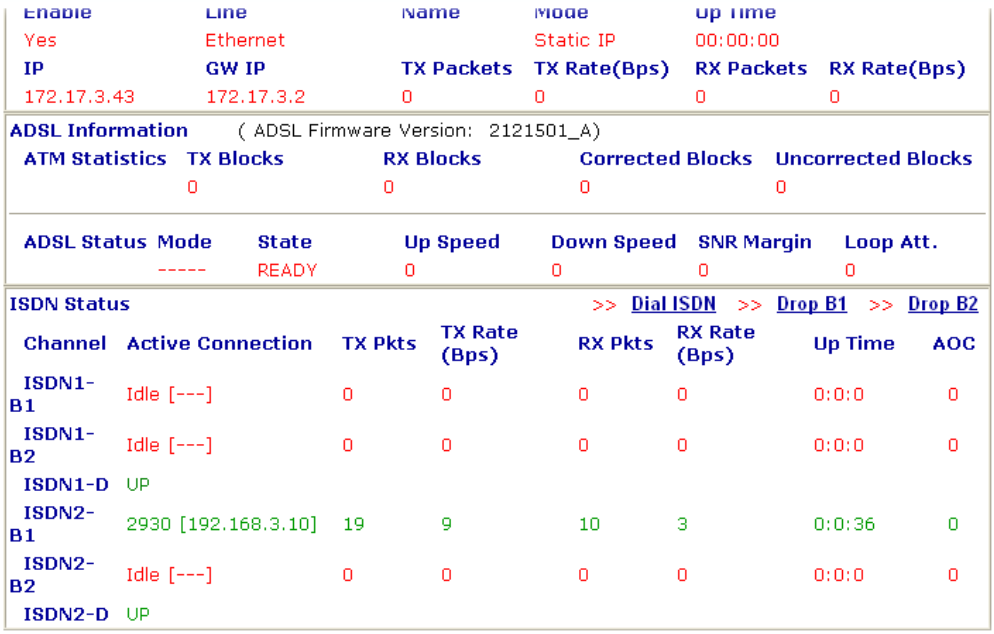
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:22	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
218.160.234.238	61.216.116.254	14	16	15	41

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	18	23	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	11936000	0	0

Online status for ISDN enabled



Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	00:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
172.17.3.43	172.17.3.2	0	0	0	0

ADSL Information (ADSL Firmware Version: 2121501_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	0	0	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	-----	READY	0	0	0	0

ISDN Status >> Dial ISDN >> Drop B1 >> Drop B2

Channel	Active Connection	TX Pkts	TX Rate (Bps)	RX Pkts	RX Rate (Bps)	Up Time	AOC
ISDN1-B1	Idle [---]	0	0	0	0	0:0:0	0
ISDN1-B2	Idle [---]	0	0	0	0	0:0:0	0
ISDN1-D	UP						
ISDN2-B1	2930 [192.168.3.10]	19	9	10	3	0:0:36	0
ISDN2-B2	Idle [---]	0	0	0	0	0:0:0	0
ISDN2-D	UP						

Detailed explanation is shown below:

Primary DNS Displays the IP address of the primary DNS.

Secondary DNS Displays the IP address of the secondary DNS.

LAN Status

IP Address Displays the IP address of the LAN interface.

TX Packets Displays the total transmitted packets at the LAN interface.

RX Packets Displays the total number of received packets at the LAN interface.

WAN1/2 Status

Line Displays the physical connection (Ethernet) of this interface.

Name Displays the name set in WAN1/WAN web page.

Mode Displays the type of WAN connection (e.g., PPPoE).

Up Time Displays the total uptime of the interface.

IP Displays the IP address of the WAN interface.

GW IP Displays the IP address of the default gateway.

TX Packets Displays the total transmitted packets at the WAN interface.

TX Rate Displays the speed of transmitted octets at the WAN interface.

RX Packets Displays the total number of received packets at the WAN interface.

RX Rate Displays the speed of received octets at the WAN interface.

ISDN Status

Channel Active Conn. Displays the active connection status for each channel.

TX Pkts Displays the total transmitted packets at the ISDN interface.

TX Rate Displays the speed of transmitted octets at the ISDN interface.

RX Pkts Displays the total number of received packets at the ISDN interface.

RX Rate	Displays the speed of received octets at the ISDN interface.
Up Time	Displays the total uptime of the interface.
AOC	Displays the charge information of the interface.

Note: The words in green mean that the WAN connection of that interface (WAN1/WAN2) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1/WAN2) is not ready for accessing Internet.

2.4 Saving Configuration

Each time you click **OK** on the web page for saving the configuration, you can find messages showing the system interaction with you.

Ready indicates the system is ready for you to input settings.

Settings Saved means your settings are saved once you click **Finish** or **OK** button.

This page is left blank.

3 Advanced Web Configuration

After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more setting for suiting his/her request, please refer to this chapter for getting detailed information about the advanced configuration of this router. As for other examples of application, please refer to chapter 4.

3.1 WAN

Quick Start Wizard offers user an easy method to quick setup the connection mode for the router. Moreover, if you want to adjust more settings for different WAN modes, please go to **WAN** group and click the **Internet Access** link.

3.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as ***private*** IP addresses, and are listed in the following ranges:

From 10.0.0.0 to 10.255.255.255
From 172.16.0.0 to 172.31.255.255
From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network. Thus, all the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This implementation provides users with significant ease of use. Meanwhile it provides access control, billing, and type of service according to user requirement.

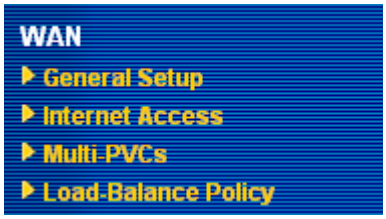
When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

3.1.2 Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor2820 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2820, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2820 with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via 802.11n wireless function of Vigor2820n, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor2820 series.

After connecting into the router, 3G USB Modem will be regarded as the second WAN port. However, the original Ethernet WAN1 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN2 also can be used as backup device. Therefore, when WAN1 is not available, the router will use 3.5G for supporting automatically. The supported 3G USB Modem will be listed on Draytek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for Internet Access.



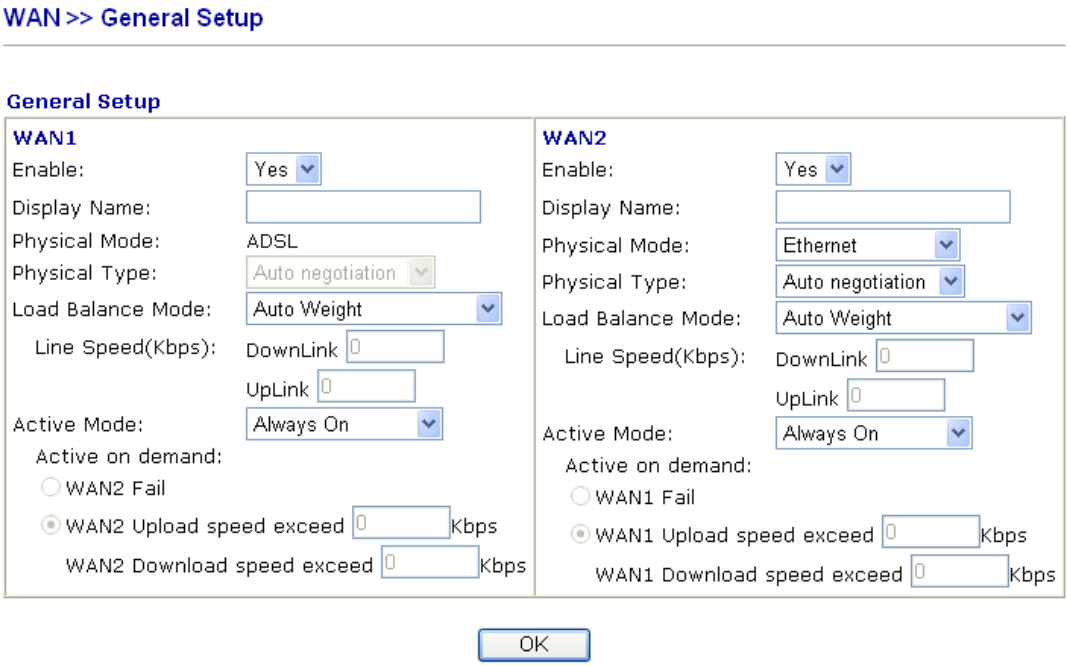
3.1.3 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 and WAN2 in details.

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

This webpage allows you to set general setup for WAN1 and WAN respectively.

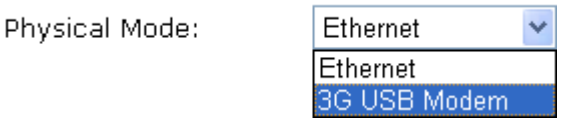
Note: In default, WAN1 and WAN2 are enabled.



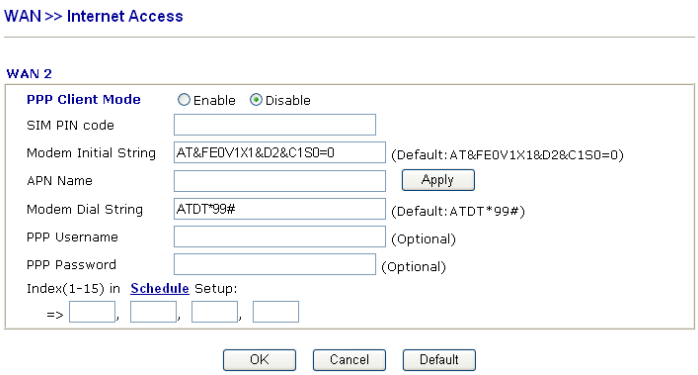
Enable Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.

Display Name Type the description for the WAN1/WAN2 interface.

Physical Mode For WAN1, the physical connection is done through ADSL port; yet the physical connection for WAN2 is done through an Ethernet port (P1) or USB port. You cannot change it.

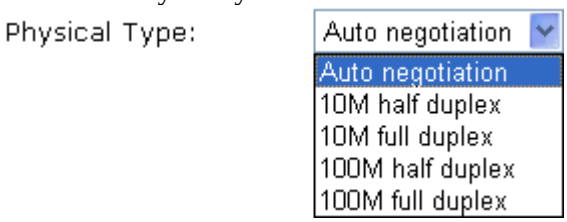


To use 3G network connection through 3G USB Modem, choose **3G USB Modem** as the physical mode in **WAN2**. Next, go to **WAN>> Internet Access**. 3G USB Modem is available for WAN2. You can enable **PPP** as the access mode and complete further configuration.



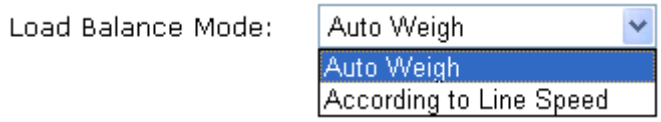
Physical Type This setting is available for WAN2 only. You can change the physical type for WAN2 or choose **Auto negotiation** for

determined by the system.



Load Balance Mode

If you know the practical bandwidth for your WAN interface, please choose the setting of **According to Line Speed**. Otherwise, please choose **Auto Weigh** to let the router reach the best load balance.

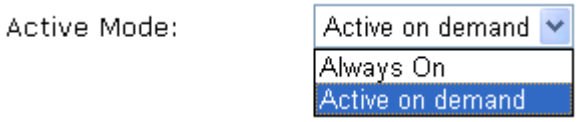


Line Speed

If your choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.

Active Mode

Choose **Always On** to make the WAN connection (WAN1/WAN2) being activated always; or choose **Active on demand** to make the WAN connection (WAN1/WAN2) activated if it is necessary.



If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes.

WAN2 Fail – It means the connection for WAN1 will be activated when WAN2 is failed.

WAN2 Upload speed exceed XX kbps – It means the connection for WAN1 will be activated when WAN2 Upload speed exceed certain value that you set in this box for 15 seconds.

WAN2 Download speed exceed XX kbps– It means the connection for WAN1 will be activated when WAN2 Download speed exceed certain value that you set in this box for 15 seconds.

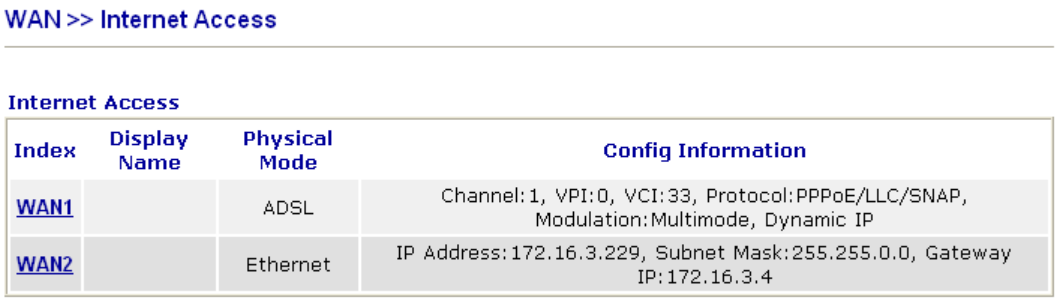
WAN1 Fail – It means the connection for WAN2 will be activated when WAN1 is failed.

WAN1 Upload speed exceed XX kbps – It means the connection for WAN2 will be activated when WAN1 Upload speed exceed certain value that you set in this box for 15 seconds.

WAN1 Download speed exceed XX kbps– It means the connection for WAN2 will be activated when WAN1 Download speed exceed certain value that you set in this box for 15 seconds.

3.1.4 Internet Access

For the router supports dual WAN function, the users can set different WAN settings (for WAN1/WAN2) for Internet Access. Due to different physical mode for WAN1 and WAN2, the Access Mode for these two connections also varies slightly.



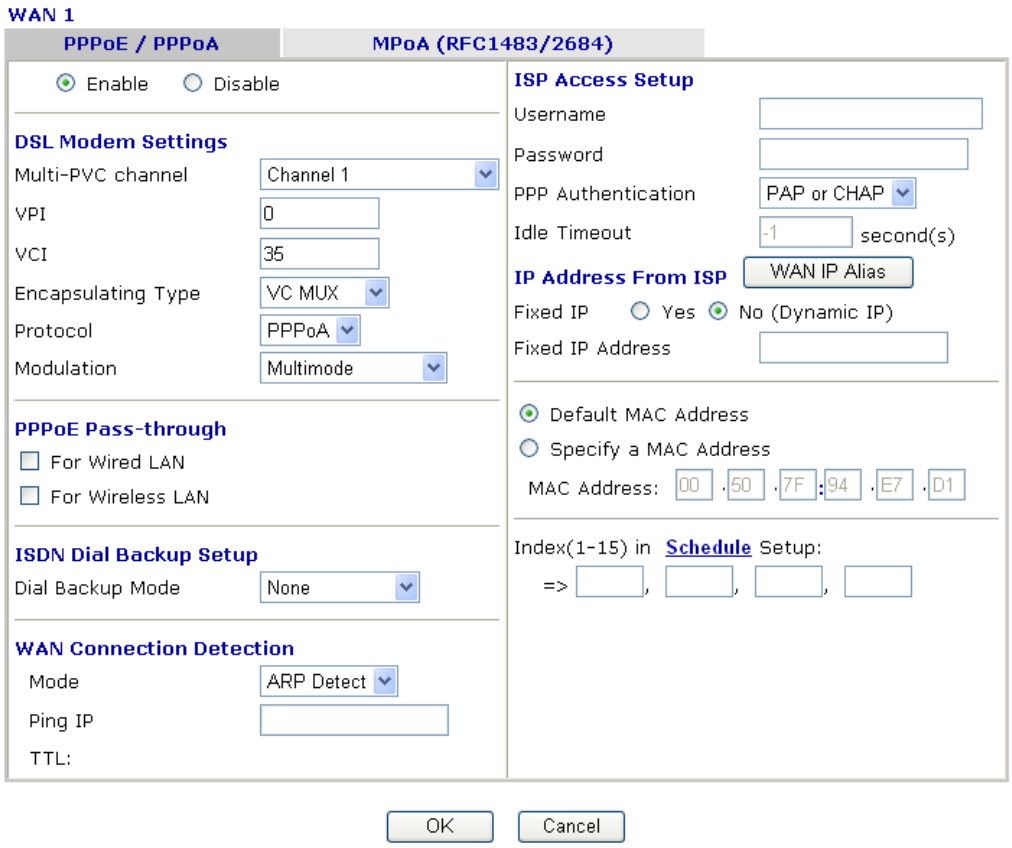
Index	It shows the WAN modes that this router supports. WAN1 is the default WAN interface for accessing into the Internet. WAN2 is the optional WAN interface for accessing into the Internet when WAN 1 is inactive for some reason.
Display Name	It shows the name of the WAN1/WAN2 that entered in general setup.
Physical Mode	It shows the physical port for WAN1/WAN2.
Config Information	It shows brief configuration information for WAN1/WAN2 interface.

WAN1 and WAN2 support different protocols. WAN1 supports PPPoE/PPPoA and MPoA. WAN2 supports PPPoE, Static or Dynamic IP and PPTP. According to physical connection of your router, please choose suitable WAN interface link to set detailed information.

PPPoE/PPPoA for WAN1

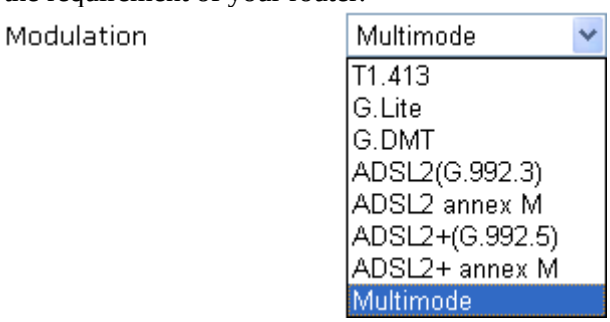
To use **PPPoE/PPPoA** as the accessing protocol of the Internet, select **PPPoE/PPPoA** mode. The following web page will appear.

WAN >> Internet Access



Enable/Disable Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

DSL Modem Settings Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
Multi-PVC channel - The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Select M-PVCs Channel** means no selection will be chosen.
VPI - Type in the value provided by ISP.
VCI - Type in the value provided by ISP.
Encapsulating Type - Drop down the list to choose the type provided by ISP.
Protocol - Drop down the list to choose the one provided by ISP. If you have already used **Quick Start Wizard** to set the protocol, then it is not necessary for you to change any settings in this group.
Modulation –Default setting is Multimode. Choose the one that fits the requirement of your router.

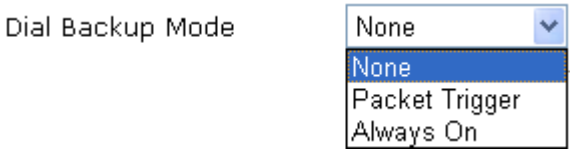


PPPoE Pass-through

The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.
For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.
For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **ISDN** > **Dialing to a Single ISP** to create the backup profile.



None - Disable the backup function.
Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

Always On - If the broadband connection is no longer available, the backup line will be activated automatically and always on until the broadband connection is restored. We recommend you to enable this feature if you host a web server for your customers' access.

This setting is available for *S* model only.

WAN Connection Detection

Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
Mode – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection.
Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

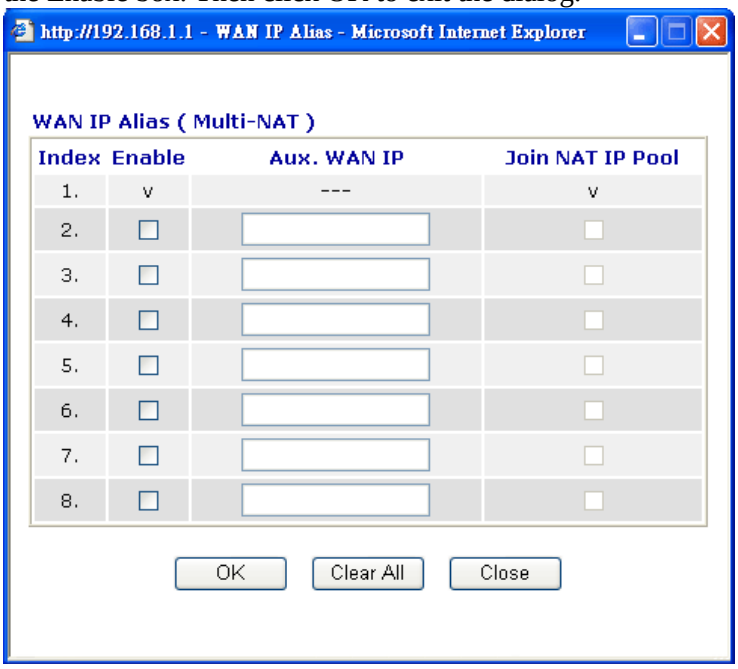
ISP Access Setup

Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.
Username – Type in the username provided by ISP in this field.
Password – Type in the password provided by ISP in this field.
PPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address From ISP

Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request.

In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.
WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



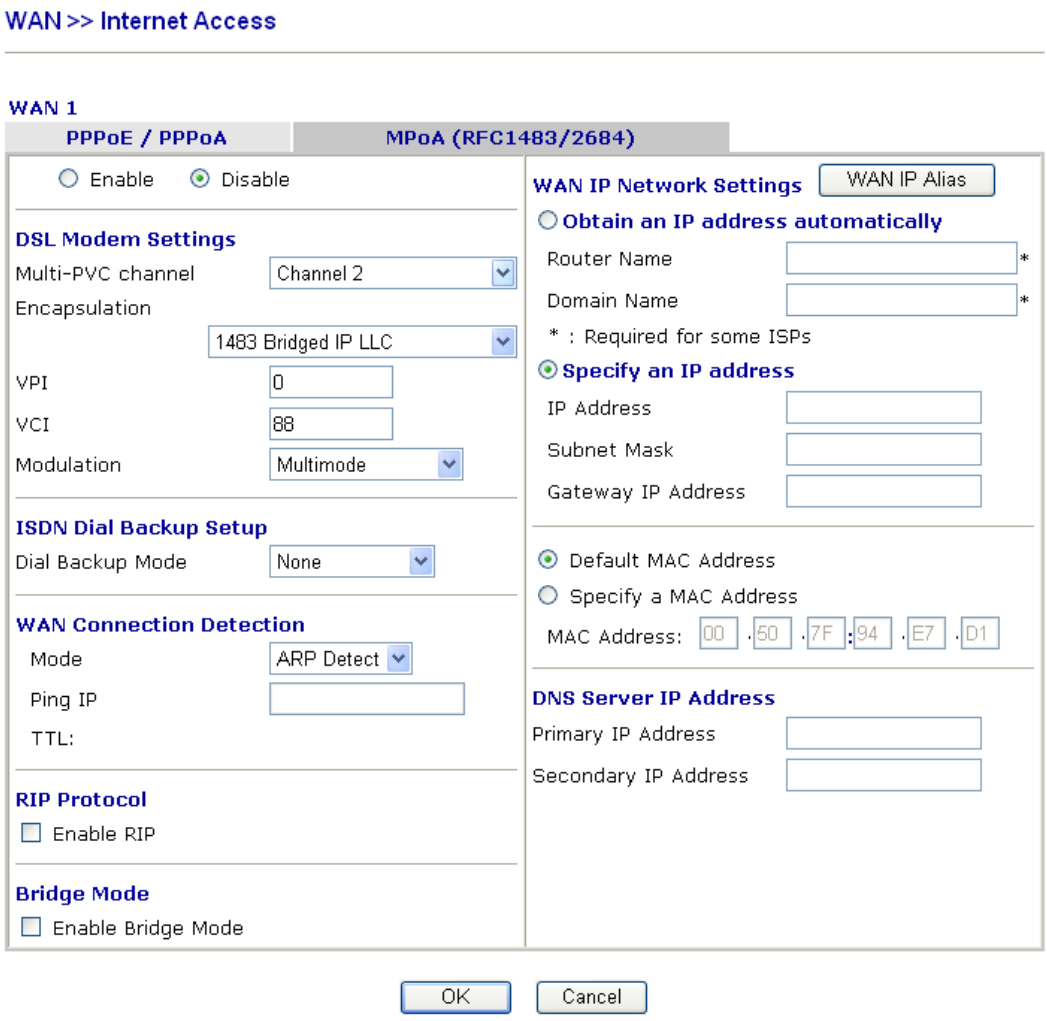
Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.
Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.
Specify a MAC Address – Type the MAC address for the router manually.
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Applications – Schedule** web page and you can use the number that you have set in that web page.

After finishing all the settings here, please click **OK** to activate them.

MPoA for WAN1

MPoA is a specification that enables ATM services to be integrated with existing LANs, which use either Ethernet, token-ring or TCP/IP protocols. The goal of MPoA is to allow different LANs to send packets to each other via an ATM backbone.

To use **MPoA** as the accessing protocol of the Internet, select **MPoA** mode. The following web page will appear.



DSL Modem Settings Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.

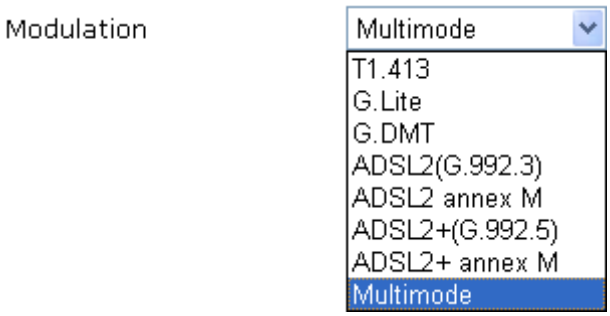
Multi-PVC channel - The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Select M-PVCs Channel** means no selection will be chosen.

Encapsulating Type - Drop down the list to choose the type provided by ISP.

VPI - Type in the value provided by ISP.

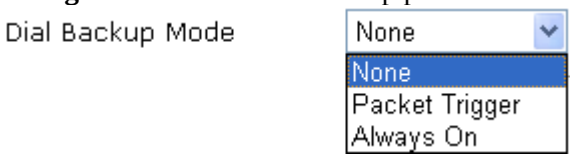
VCI - Type in the value provided by ISP.

Modulation –Default setting is Multimode. Choose the one that fits the requirement of your router.



ISDN Dial Backup Setup This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **ISDN** > **Dialing to**

a Single ISP to create the backup profile.



None - Disable the backup function.
Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

Always On - If the broadband connection is no longer available, the backup line will be activated automatically and always on until the broadband connection is restored. We recommend you to enable this feature if you host a web server for your customers' access.

This setting is available for *n* model only.

WAN Connection Detection

Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
Mode – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection.
Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

RIP Protocol

Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.

Bridge Mode

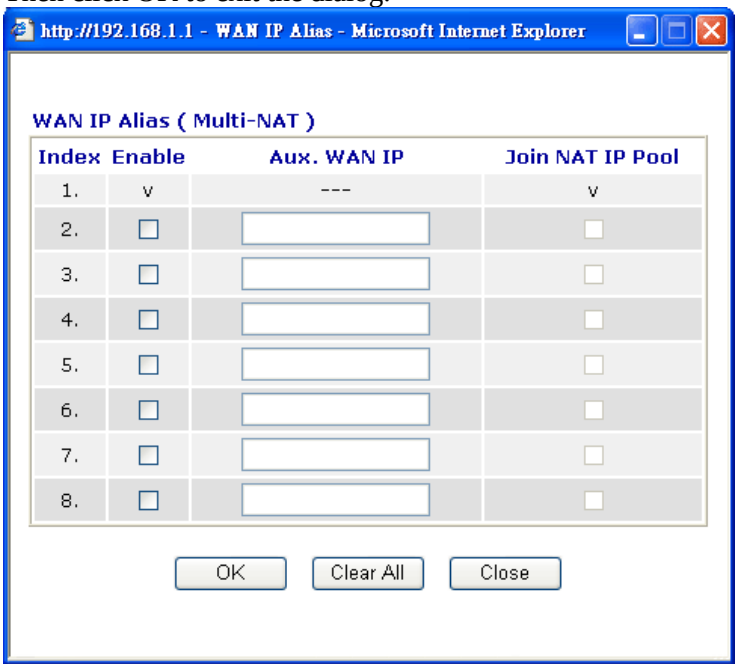
If you choose **Bridged IP** as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.

WAN IP Network Settings

This group allows you to obtain an IP address automatically and allows you type in IP address manually.

Obtain an IP address automatically – Click this button to obtain the IP address automatically.
Router Name – Type in the router name provided by ISP.
Domain Name – Type in the domain name that you have assigned.
Specify an IP address – Click this radio button to specify some data.
WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box.

Then click OK to exit the dialog.



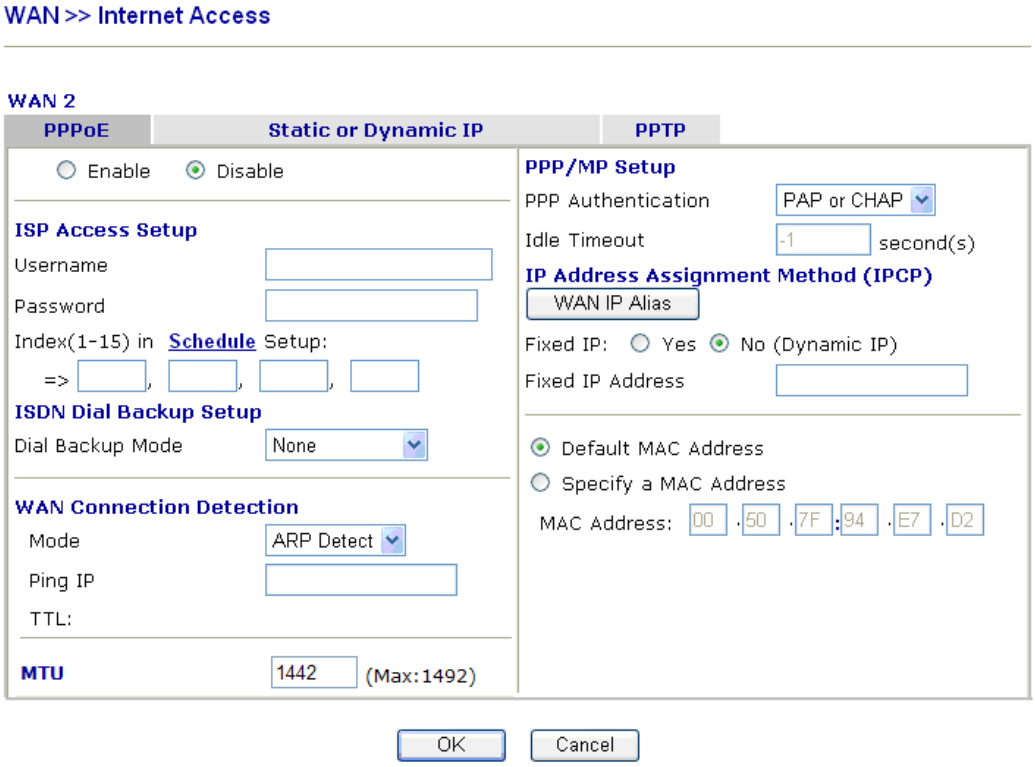
IP Address – Type in the private IP address.
Subnet Mask – Type in the subnet mask.
Gateway IP Address – Type in gateway IP address.
Default MAC Address Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity.
MAC Address – Type in the MAC address for the router manually.

DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

After finishing all the settings here, please click **OK** to activate them.

PPPoE for WAN2

To use **PPPoE** as the accessing protocol of the Internet, select **PPPoE** mode. The following web page will appear.



Enable/Disable

Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

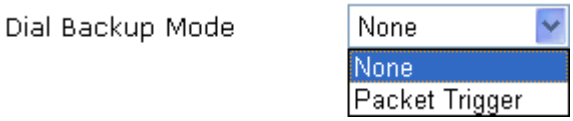
ISP Access Setup

Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.

Username – Type in the username provided by ISP in this field.
Password – Type in the password provided by ISP in this field.
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **ISDN** > **Dialing to a Single ISP** to create the backup profile.



None - Disable the backup function.
Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

This setting is available for *s* model only.

WAN Connection Detection

Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
Mode – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection.

Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

MTU

Mean maximum transmission unit of one packet. The default value is 1442.

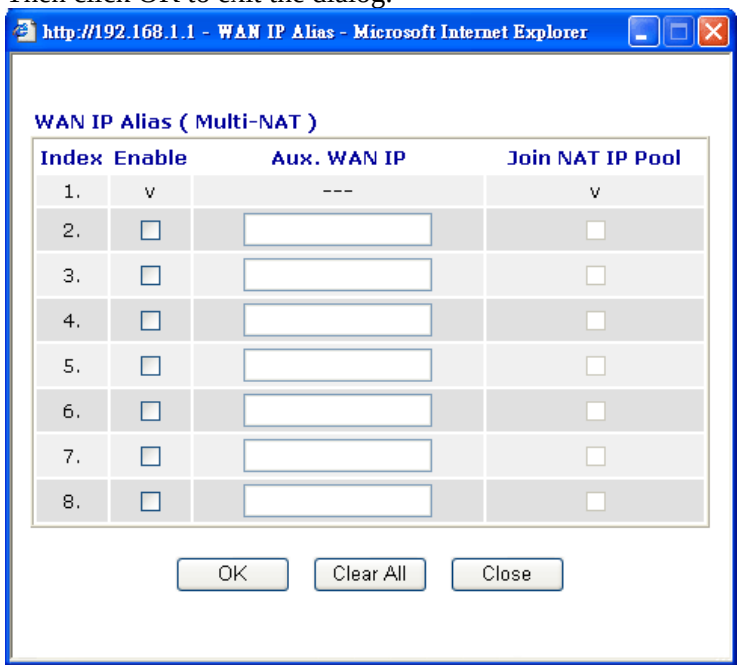
PPP/MP Setup

PPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address Assignment Method (IPCP)

Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



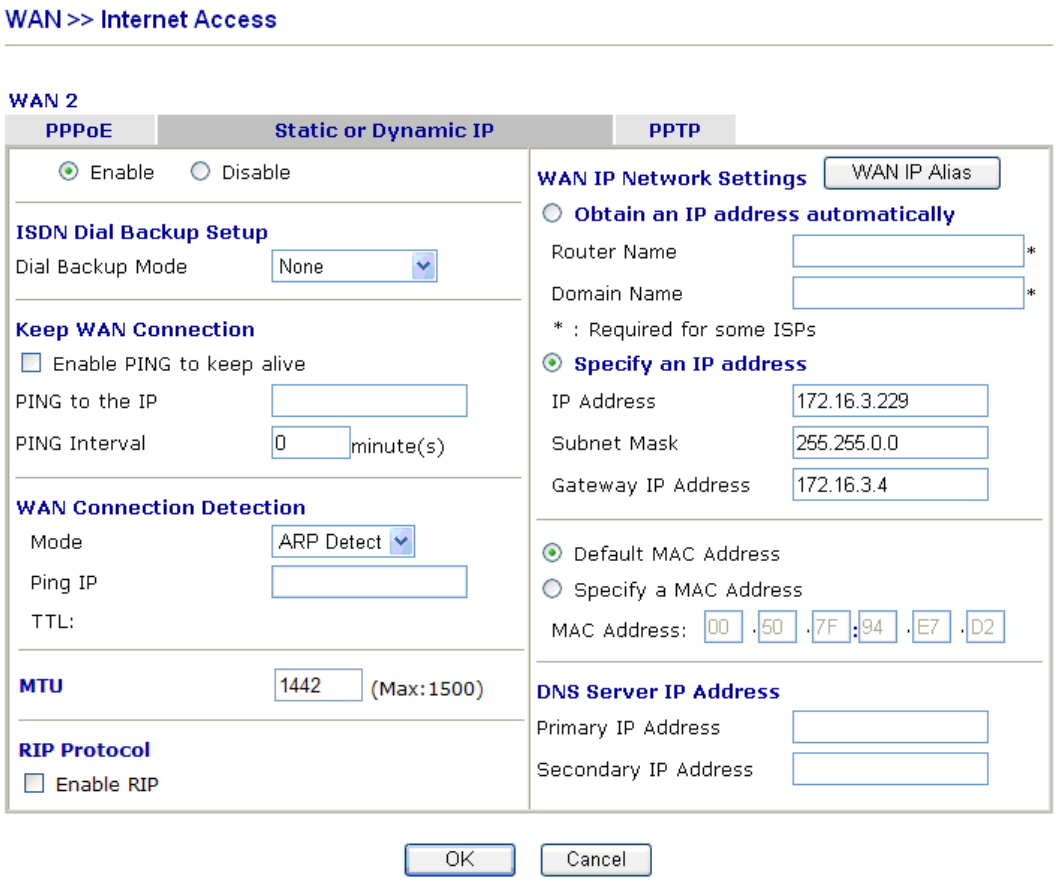
Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.
Fixed IP Address -Type a fixed IP address.
Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.
Specify a MAC Address – Type the MAC address for the router manually.

After finishing all the settings here, please click **OK** to activate them.

Static or Dynamic IP for WAN2

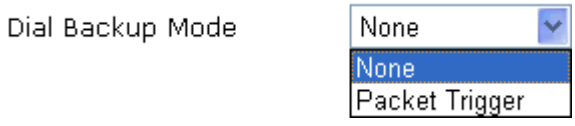
For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

To use static or dynamic IP as the accessing protocol of the Internet, select **Static or Dynamic IP** mode. The following web page will appear.



Enable/ Disable — Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

ISDN Dial Backup Setup — This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **ISDN** > **Dialing to a Single ISP** to create the backup profile.

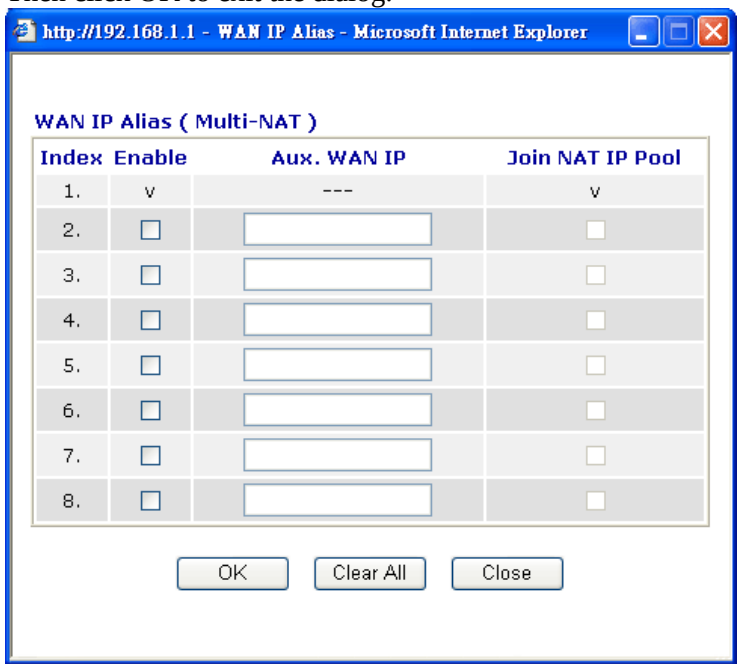


None - Disable the backup function.
Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

This setting is available for *n* model only.

WAN Connection — Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.

Detection	**Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function. **PING to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. **PING Interval** - Enter the interval for the system to execute the PING operation.
MTU	Mean maximum transmission unit of one packet. The default value is 1442.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually. **WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



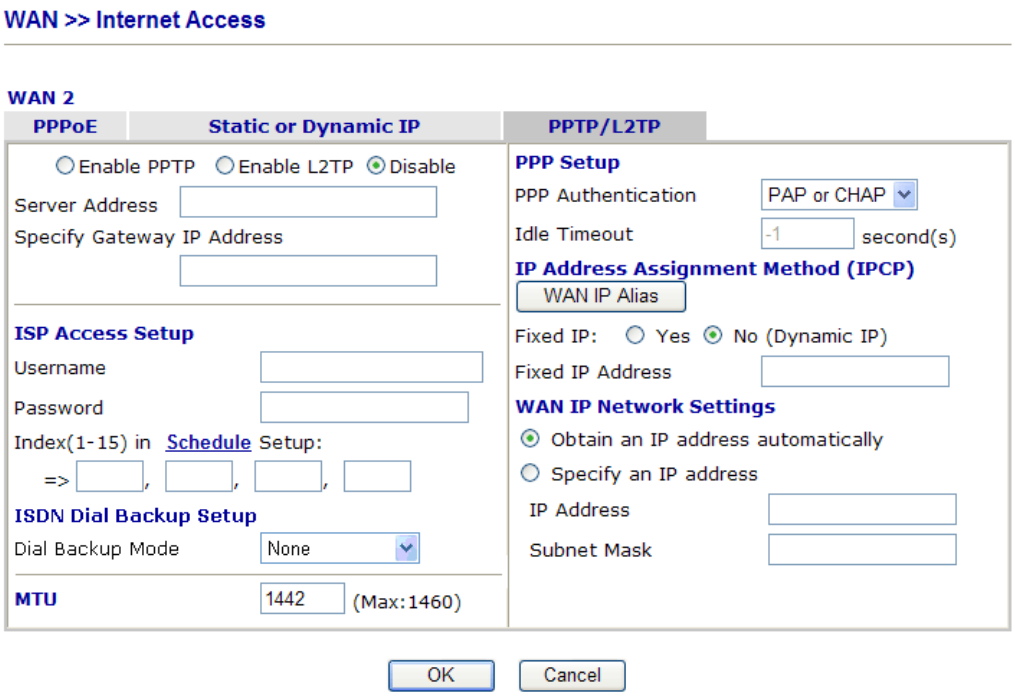
Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.
Router Name: Type in the router name provided by ISP.
Domain Name: Type in the domain name that you have assigned.
Specify an IP address – Click this radio button to specify some data

if you want to use **Static IP** mode.
IP Address: Type the IP address.
Subnet Mask: Type the subnet mask.
Gateway IP Address: Type the gateway IP address.
Default MAC Address: Click this radio button to use default MAC address for the router.
Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

DNS Server IP Address — Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

PPTP for WAN2

To use **PPTP** as the accessing protocol of the Internet, select **PPTP** mode. The following web page will appear.



Enable PPTP
Enable L2TP
Disable — Click **Enable PPTP/Enable L2TP** for activating the mode. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.

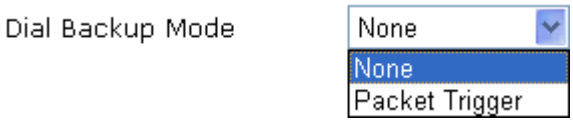
Server Address — Specify the IP address of the PPTP server.

Specify Gateway IP Address — Specify the Gateway IP address of the PPTP server.

ISP Access Setup — **Username** -Type in the username provided by ISP in this field.
Password -Type in the password provided by ISP in this field.
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **ISDN** > **Dialing to a Single ISP** to create the backup profile.



None - Disable the backup function.
Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

This setting is available for *s* model only.

MTU

Mean maximum transmission unit of one packet. The default value is 1442.

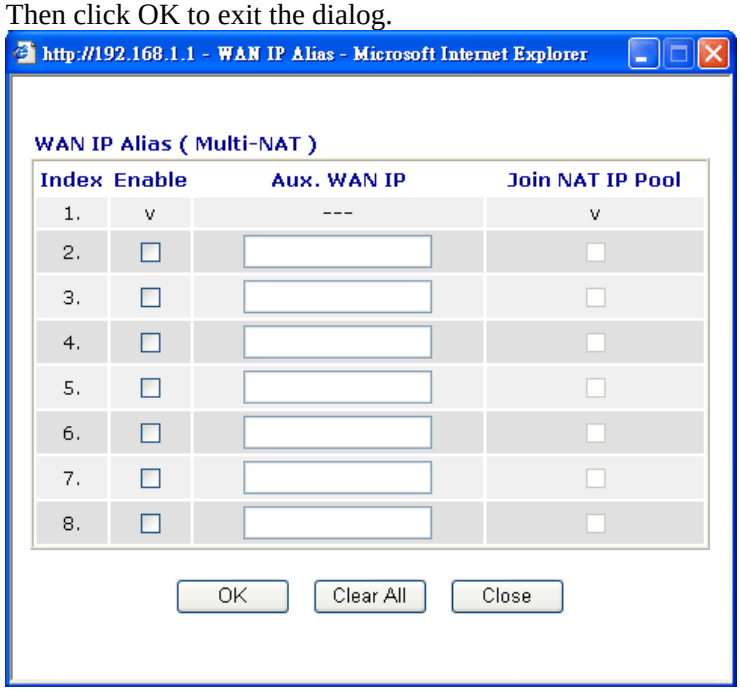
PPP Setup

PPP Authentication - Select **PAP only** or **PAP or CHAP** for PPP.
Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address Assignment Method(IPCP)

Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



Click **Yes** to use this function and type in a fixed IP address in the box.
Fixed IP - Click **Yes** to use this function and type in a fixed IP

address in the box of **Fixed IP Address**.
Fixed IP Address -Type a fixed IP address.

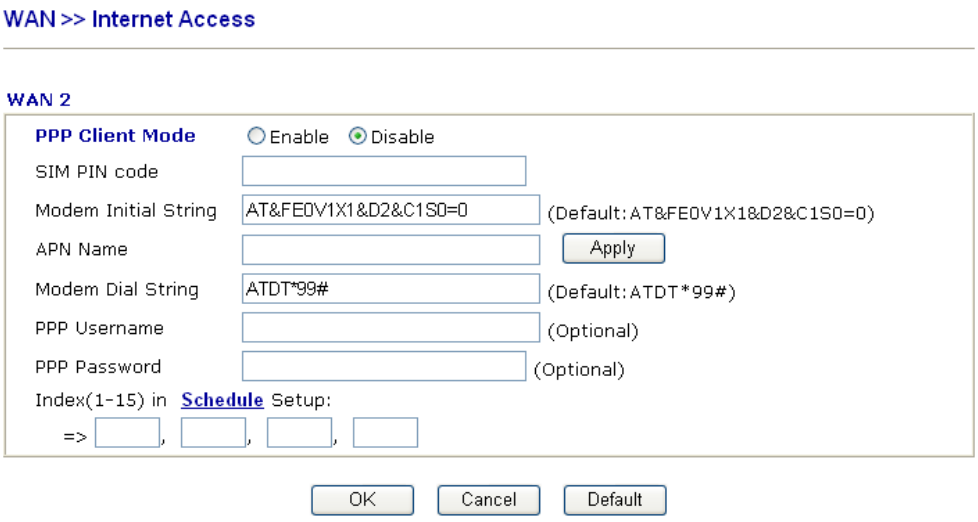
WAN IP Network Settings

Obtain an IP address automatically – Click this button to obtain the IP address automatically.

Specify an IP address – Click this radio button to specify some data.
IP Address – Type the IP address.
Subnet Mask – Type the subnet mask.

PPP for WAN2

Such mode is active only **3G USB Modem** was chosen as the physical mode in General Setup.



PPP Client Mode Click Enable to activate this mode for WAN2.

SIM PIN code Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name APN(Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting.
Apply – Activate the function of identification.

Modem Dial String Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username Type the PPP username (optional).

PPP Password Type the PPP password (optional).

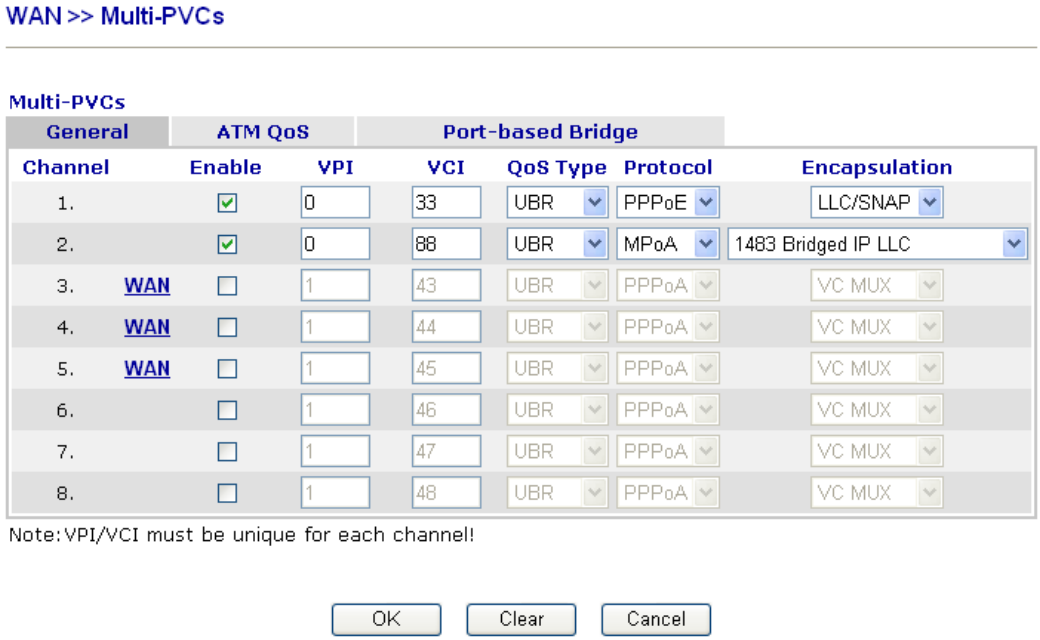
Index (1-15) Set the PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Schedule** setup. The default setting of this filed is blank and the function will always work.

3.1.5 Multi-PVCs

This router allows you to create multi-PVCs for different data transferring for using. Simply go to **Internet Access** and select **Multi-PVC Setup** page.

General

The system allows you to set up to eight channels which are ready for choosing as the first PVC line that will be used as multi-PVCs.

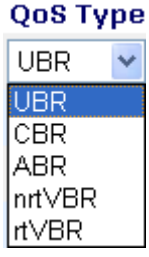


Enable Check this box to enable that channel. The channels that you enabled here will be shown in the **Multi-PVC channel** drop down list on the web page of **Internet Access**. Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of **Internet Access**.

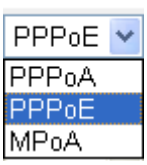
VPI Type in the value provided by your ISP.

VCI Type in the value provided by your ISP.

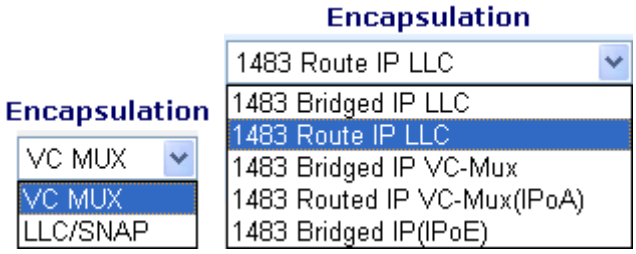
QoS Type Select a proper QoS type for the channel.



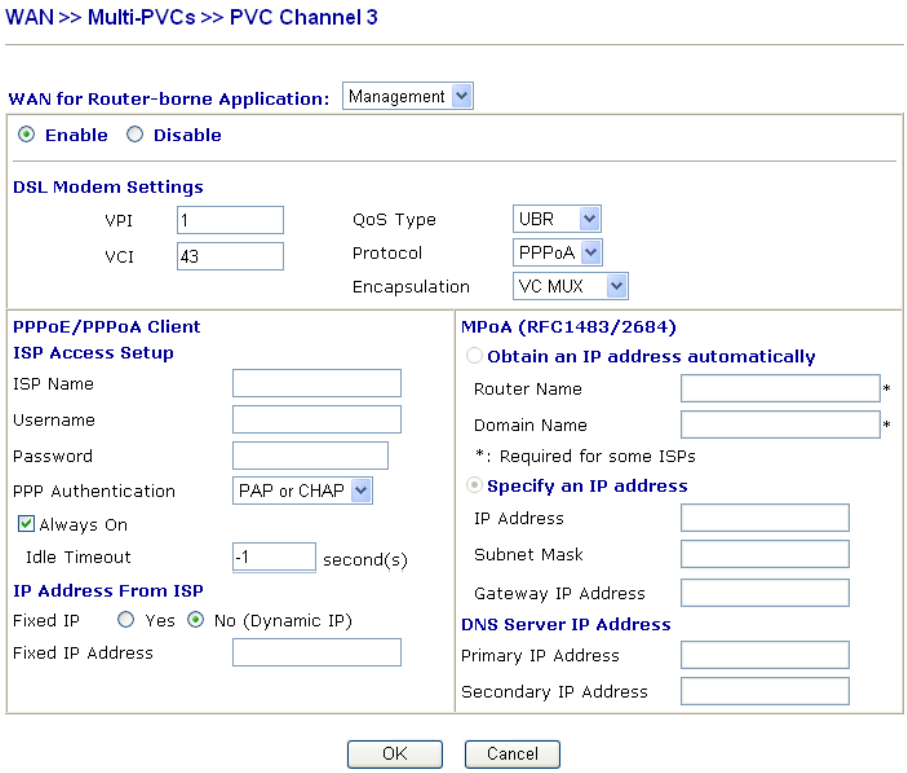
Protocol Select a proper protocol for this channel.



Encapsulation Choose a proper type for this channel. The types will be different according to the protocol setting that you choose.

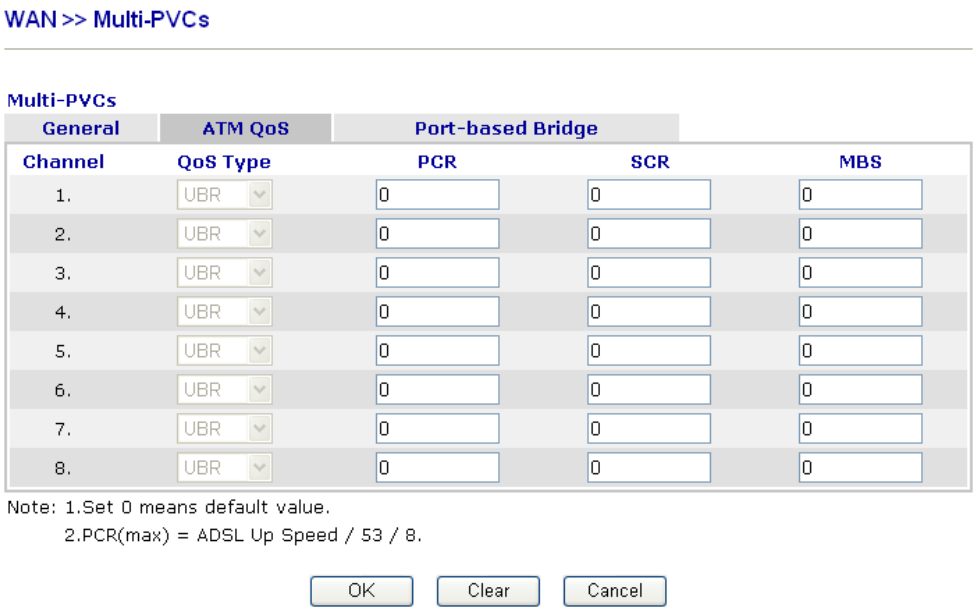


WAN link for Channel 3, 4, 5 are provided for router-borne application such as TR069 and VoIP. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 3, 4 or 5 to configure your router.

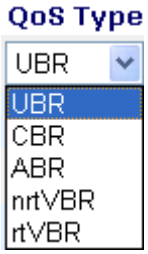


ATM QoS

Such configuration is applied to upstream packets. Such information will be provided by ISP. Please contact with your ISP for detailed information.



QoS Type Select a proper QoS type for the channel according to the information that your ISP provides.



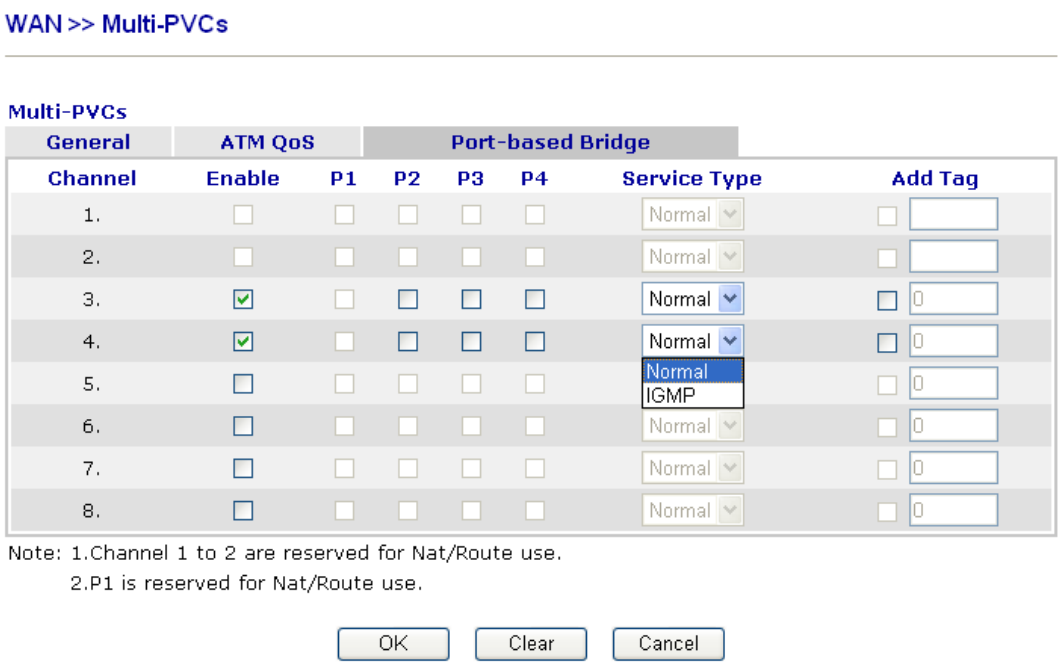
PCR It represents Peak Cell Rate. The default setting is “0”.

SCR It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.

MBS It represents Maximum Burst Size. The range of the value is 10 to 50.

Port-based Bridge

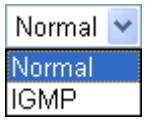
General page lets you set the first PVC. As to set the second PVC line, please click the **Port-based Bridge** tab to open Bridge configuration page.



Enable — Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 4 are reserved for NAT using.

P1 to P4 — It means the LAN port 1 to 4. Check the box to designate the LAN port for channel 3 to 8.

Service Type — Normally, service type is used for the service of video stream (e.g., IPTV). It can divide the packets from remote control and from video stream into different PVC. In general, the protocol used by remote control is IGMP.



Normal – It means that the PVC can accept all packets except IGMP.
IGMP – It means that the PVC can accept packets of IGMP only.

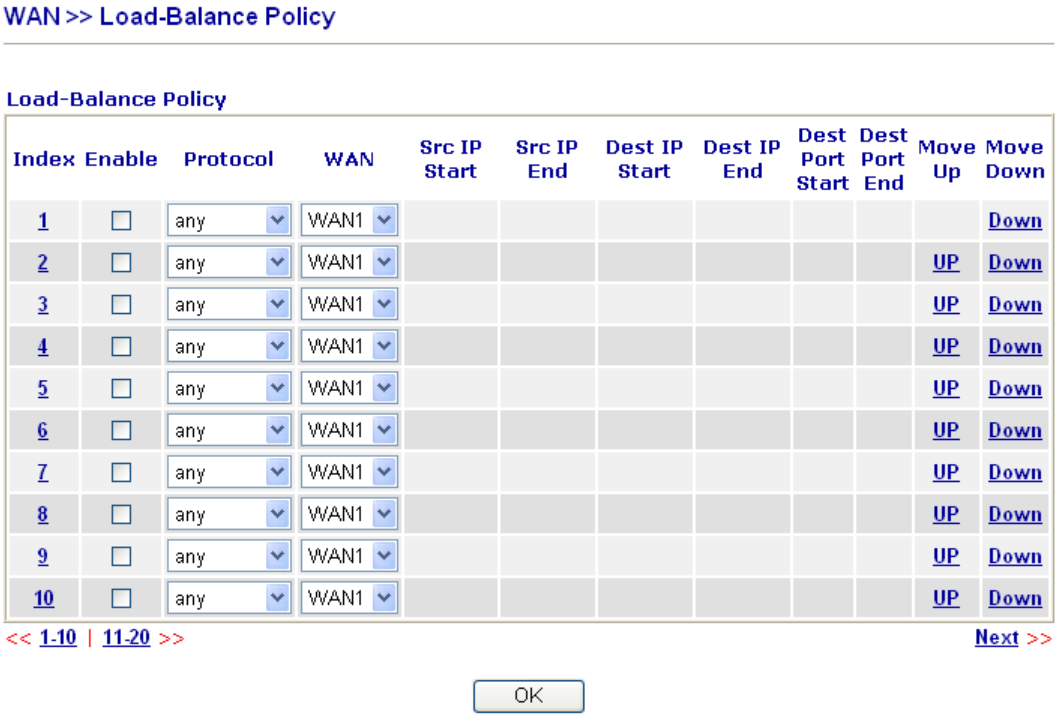
Add Tag — To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).

Click **Clear** to remove all the configurations in this page if you do not satisfy it. When you finish the configuration, please click **OK** to save and exit this page. Or click Cancel to abort the configuration and exit this page.

3.1.6 Load-Balance Policy

This router supports the function of load balancing. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN1 or WAN2 interface. The user can assign traffic category and force it to go to dedicate network interface based on the following web page setup. Twenty policies of load-balance are supported by this router.

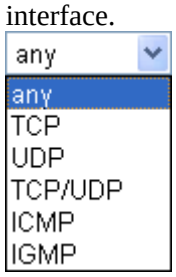
Note: Load-Balance Policy is running only when both WAN1 and WAN2 are activated.


WAN >> Load-Balance Policy
Load-Balance Policy
Index Enable Protocol WAN Src IP Start Src IP End Dest IP Start Dest IP End Dest Port Start Dest Port End Move Up Move Down
1 any WAN1 Down
2 any WAN1 UP Down
3 any WAN1 UP Down
4 any WAN1 UP Down
5 any WAN1 UP Down
6 any WAN1 UP Down
7 any WAN1 UP Down
8 any WAN1 UP Down
9 any WAN1 UP Down
10 any WAN1 UP Down
<< 1-10 | 11-20 >>
Next >>
OK

Index Click the number of index to access into the load-balance policy configuration web page.

Enable Check this box to enable this policy.

Protocol Use the drop-down menu to change the protocol for the WAN interface.



WAN Use the drop-down menu to change the WAN interface.

Src IP Start Displays the IP address for the start of the source IP.

Src IP End Displays the IP address for the end of the source IP.

Dest IP Start Displays the IP address for the start of the destination IP.

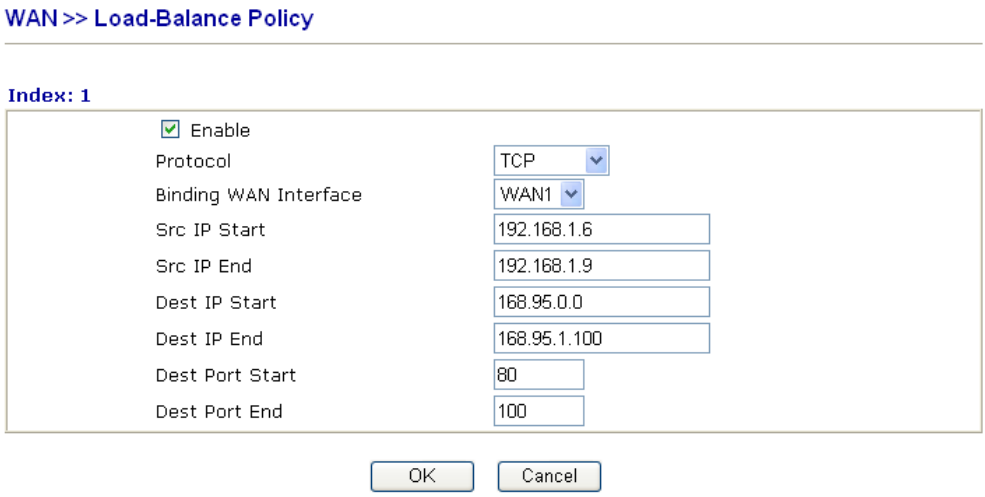
Dest IP End Displays the IP address for the end of the destination IP.

Dest Port Start Displays the IP address for the start of the destination port.

Dest Port End Displays the IP address for the end of the destination port.

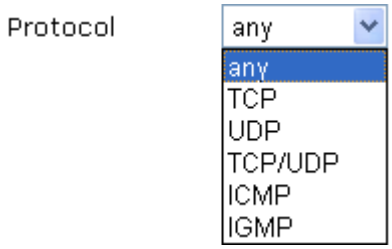
Move UP/Move Down Use **Up** or **Down** link to move the order of the policy.

Click **Index 1** to access into the following page for configuring load-balance policy.



Enable Check this box to enable this policy.

Protocol Use the drop-down menu to choose a proper protocol for the WAN interface.



Binding WAN interface Choose the WAN interface (WAN1 or WAN2) for binding.

Src IP Start Type the source IP start for the specified WAN interface.

Src IP End Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.

Dest IP Start Type the destination IP start for the specified WAN interface.

Dest IP End Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.

Dest Port Start Type the destination port start for the destination IP.

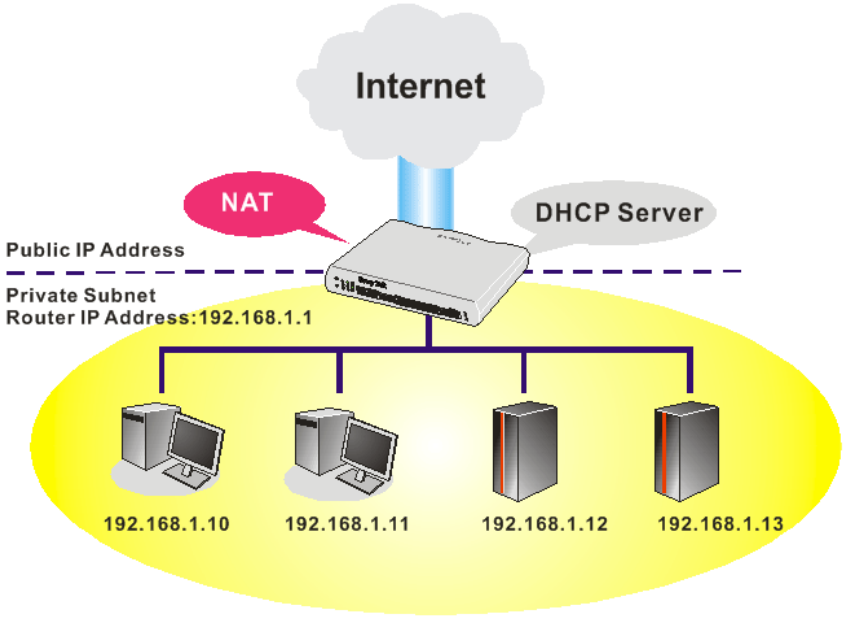
Dest Port End	Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

3.2 LAN

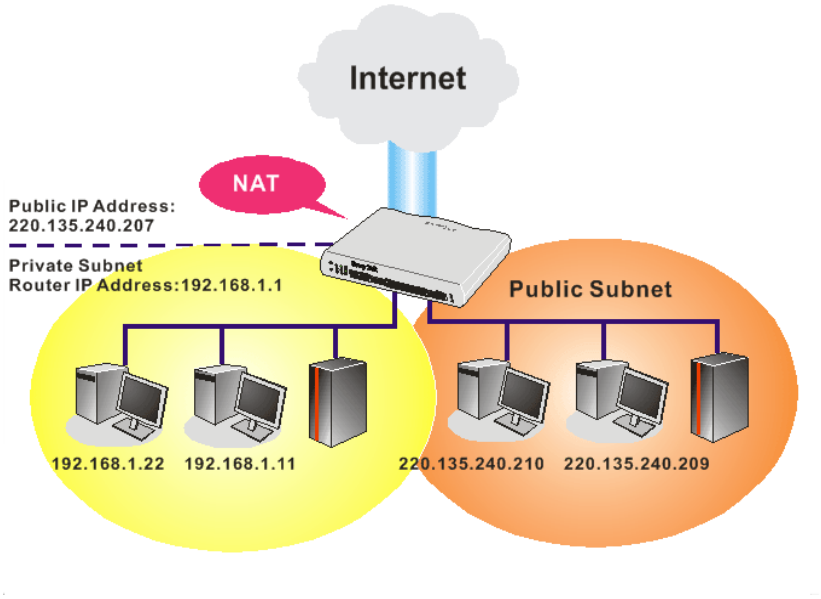
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

3.2.1 Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.



What is Routing Information Protocol (RIP)

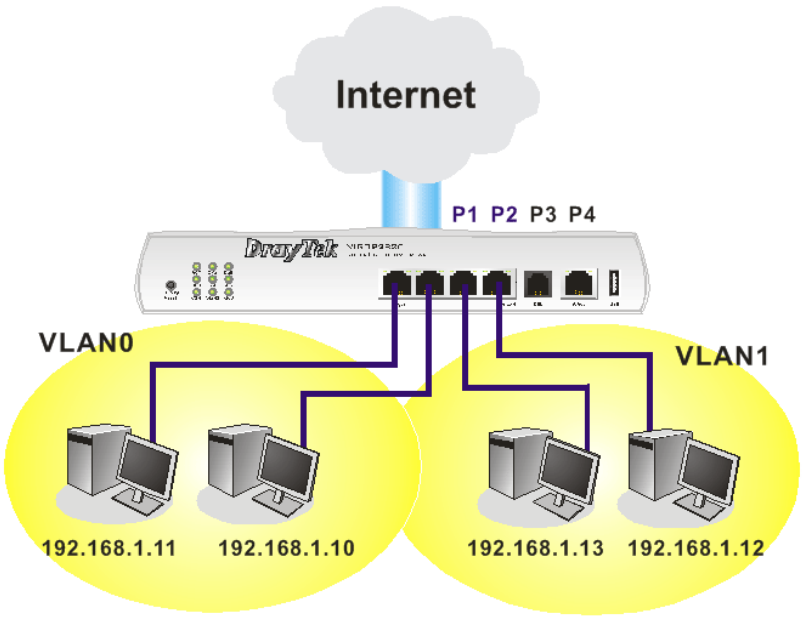
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.

What are Virtual LANs

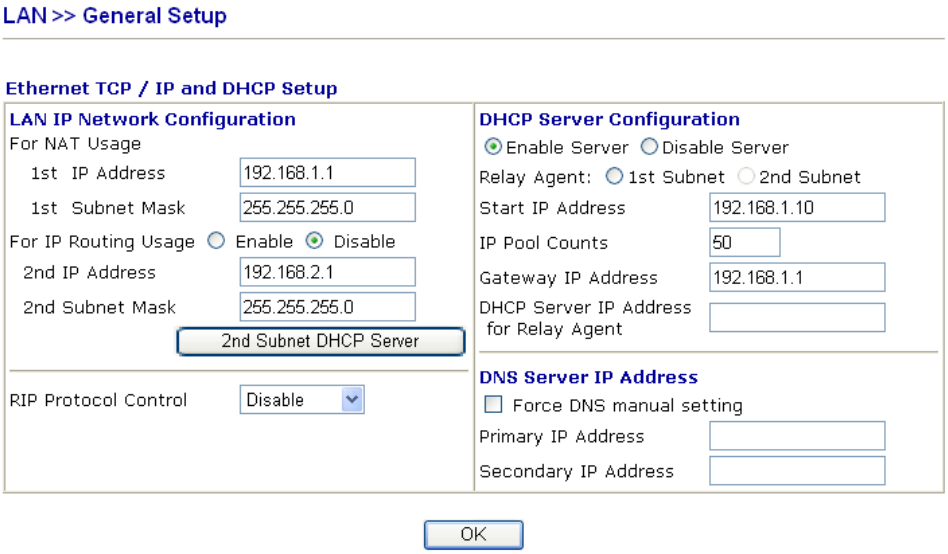
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



3.2.2 General Setup

This page provides you the general settings for LAN.

Click **LAN** to open the LAN settings page and choose **General Setup**.



1st IP Address Type in private IP address for connecting to a local private network (Default: 192.168.1.1).

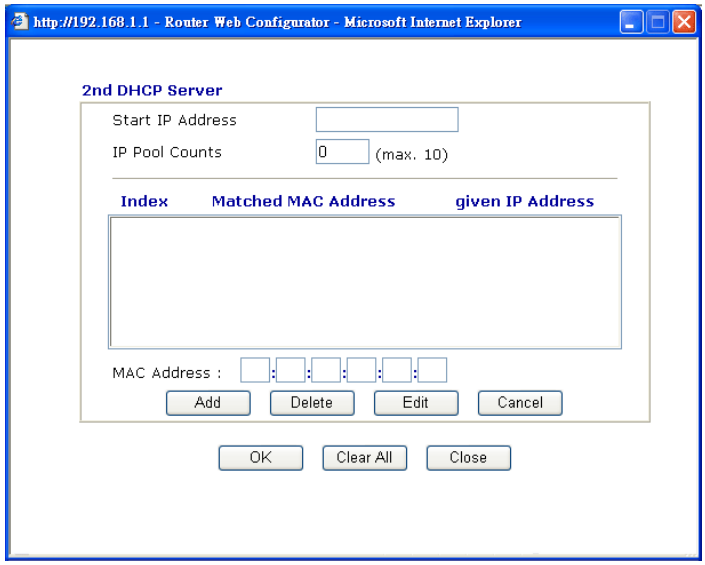
1st Subnet Mask Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

For IP Routing Usage Click **Enable** to invoke this function. The default setting is **Disable**.

2nd IP Address Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/ 24)

2nd Subnet Mask An address code that determines the size of the network. (Default: 255.255.255.0/ 24)

2nd DHCP Server You can configure the router to serve as a DHCP server for the 2nd subnet.



Start IP Address: Enter a value of the IP address pool for the DHCP

server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

MAC Address: Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

RIP Protocol Control

Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.
2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.

DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address to every host in the LAN.
Relay Agent – (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
DHCP Server IP Address for Relay Agent - Set the IP address of

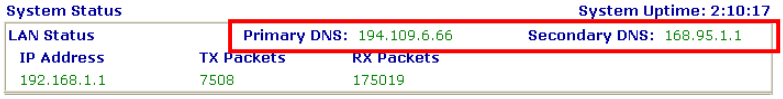
the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

The default DNS Server IP address can be found via Online Status:



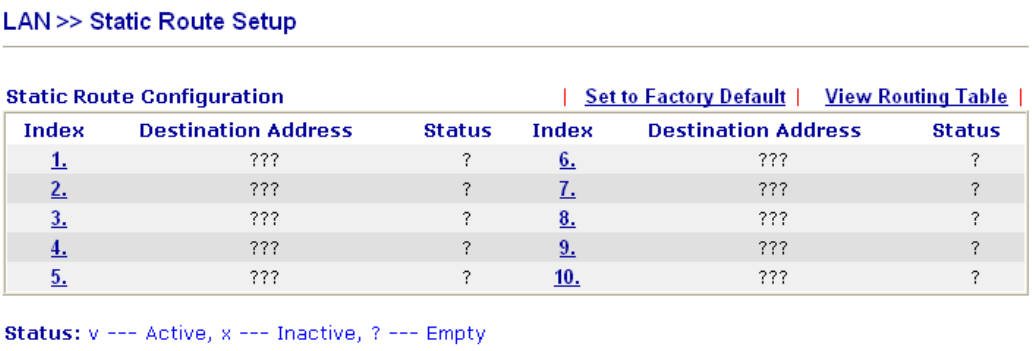
If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

There are two common scenarios of LAN settings that stated in Chapter 4. For the configuration examples, please refer to that chapter to get more information for your necessity.

3.2.3 Static Route

Go to **LAN** to open setting page and choose **Static Route**.

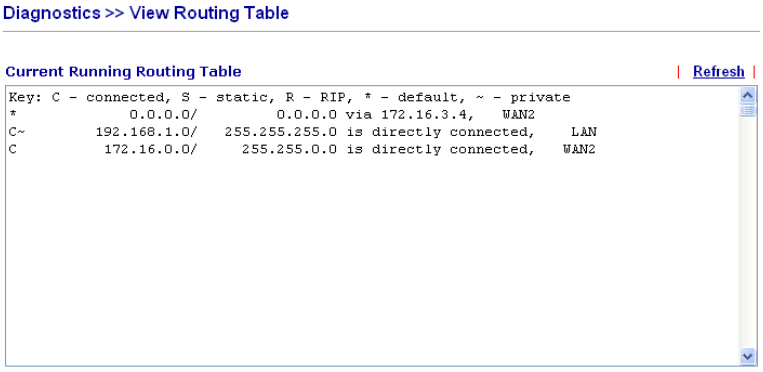


Index The number (1 to 10) under Index allows you to open next page to set up static route.

Destination Address Displays the destination address of the static route.

Status Displays the status of the static route.

Viewing Routing Table Displays the routing table for your reference.

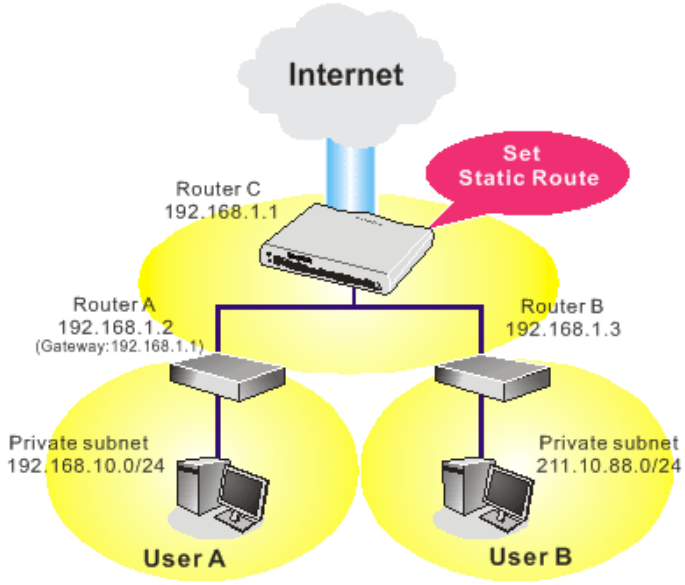

Diagnostics >> View Routing Table
Current Running Routing Table
Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private
* 0.0.0.0/ 0.0.0.0 via 172.16.3.4, WAN2
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN
C 172.16.0.0/ 255.255.0.0 is directly connected, WAN2

Add Static Routes to Private and Public Networks

Here is an example of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- use the Main Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.

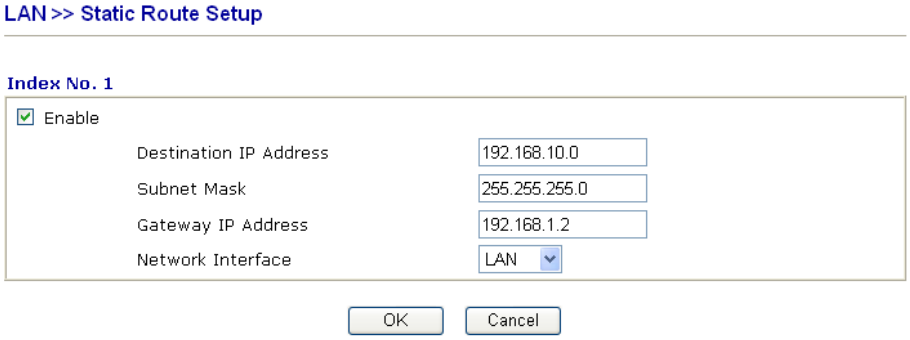


1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

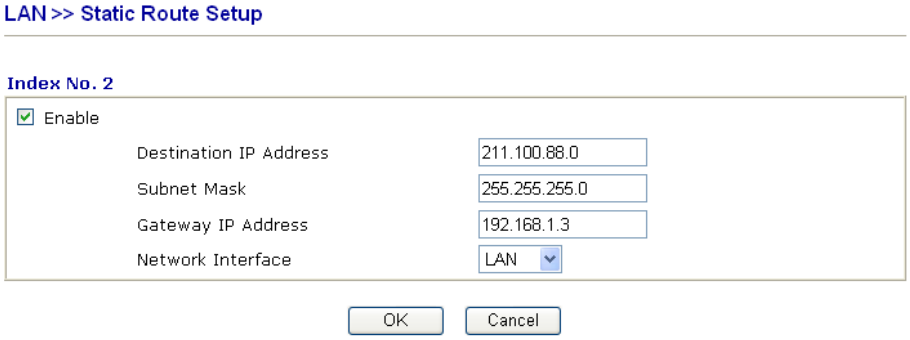
> **Note:** There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can access the Internet via

the router, and continuously exchange of IP routing information with different subnets.

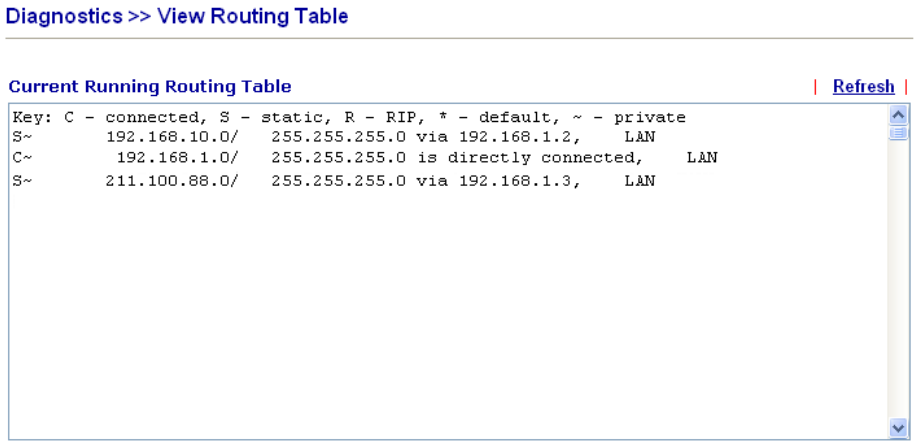
2. Click the **LAN - Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



3. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.3.

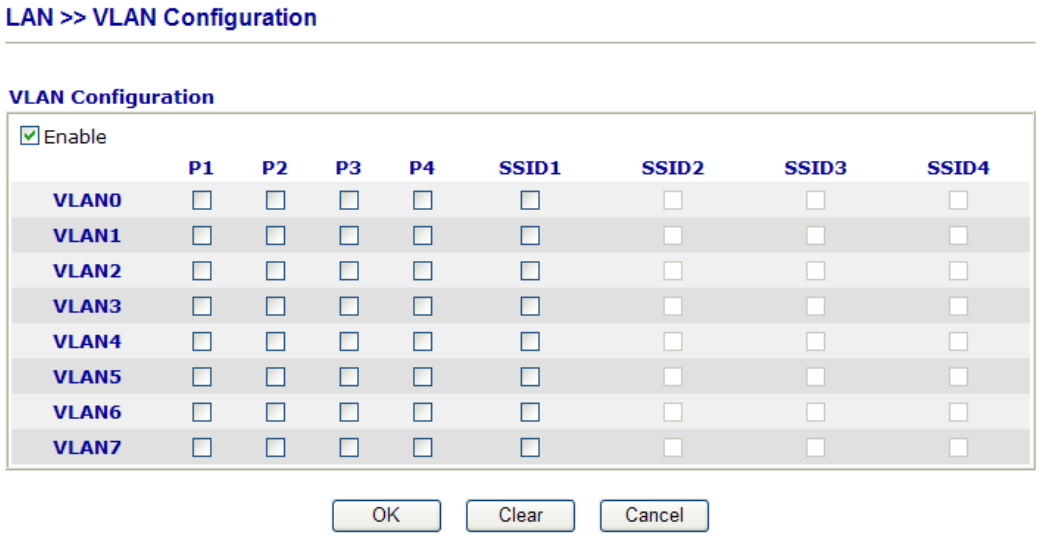


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.


Diagnostics >> View Routing Table
Current Running Routing Table
Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private
S~ 192.168.10.0/ 255.255.255.0 via 192.168.1.2, LAN
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN
S~ 211.100.88.0/ 255.255.255.0 via 192.168.1.3, LAN

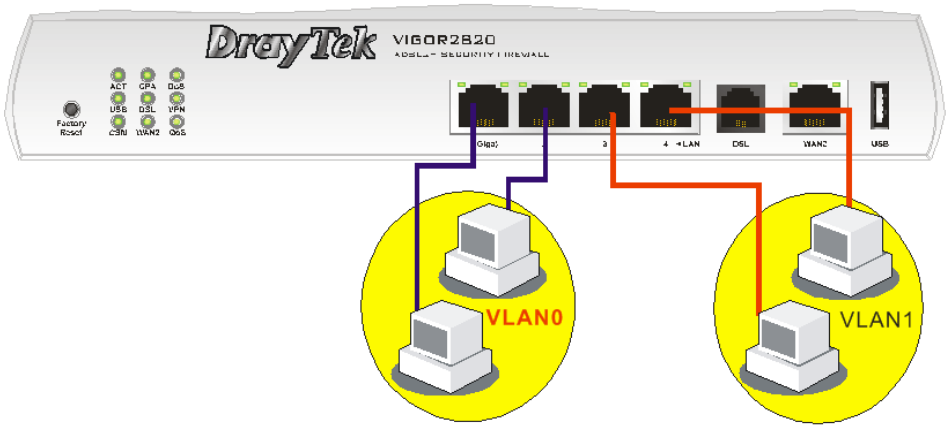
3.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

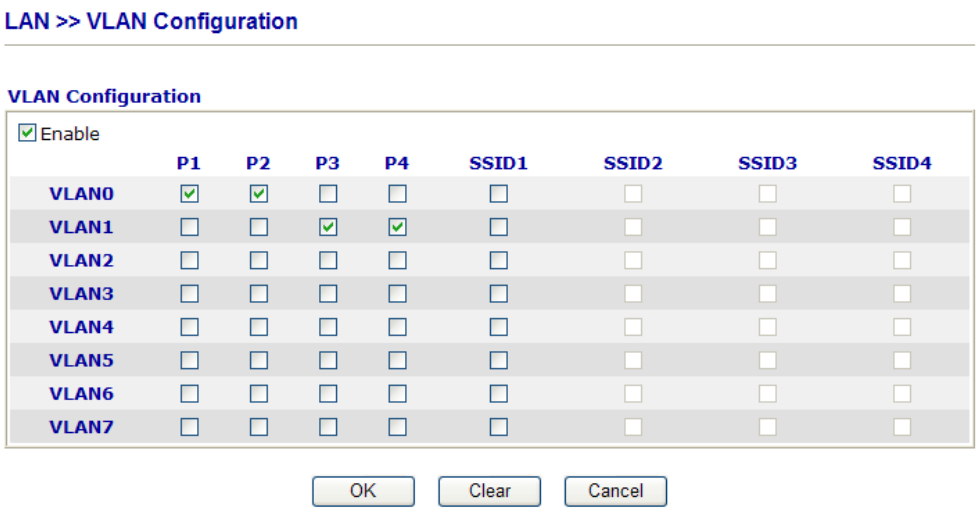


To add or remove a VLAN, please refer to the following example.

1. If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4.



2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below.

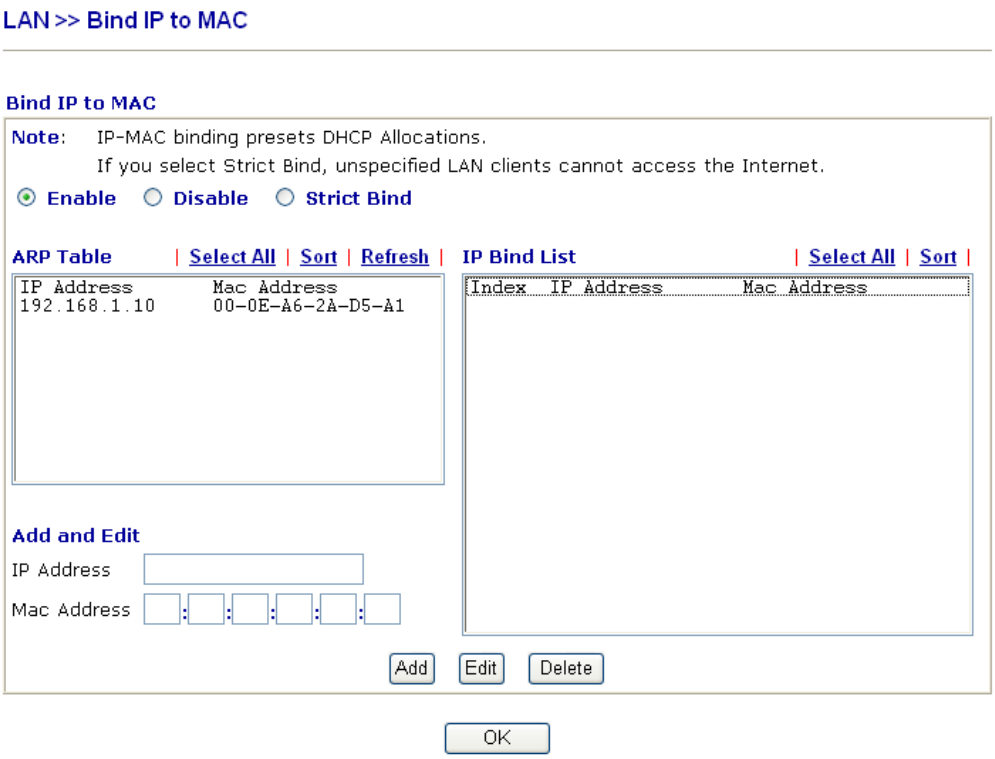


To remove VLAN, uncheck the needed box and click **OK** to save the results.

3.2.5 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. When this function is enabled, all the assigned IP and MAC address binding together cannot be changed. If you modified the binding IP or MAC address, it might cause you not access into the Internet.

Click **LAN** and click **Bind IP to MAC** to open the setup page.



Enable Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.

Disable Click this radio button to disable this function. All the settings on this page will be invalid.

Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.
Add and Edit	**IP Address** – Type the IP address that will be used for the specified MAC address. **Mac Address** – Type the MAC address that is used to bind with the assigned IP address.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in **Add and Edit** to the table of **IP Bind List**.
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Remove	You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Remove**. The selected item will be removed from the **IP Bind List**.

Note: Before you select **Strict Bind**, you have to bind one set of IP/MAC address for one PC. If not, no one of the PCs can access into Internet. And the web configurator of the router might not be accessed.

3.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

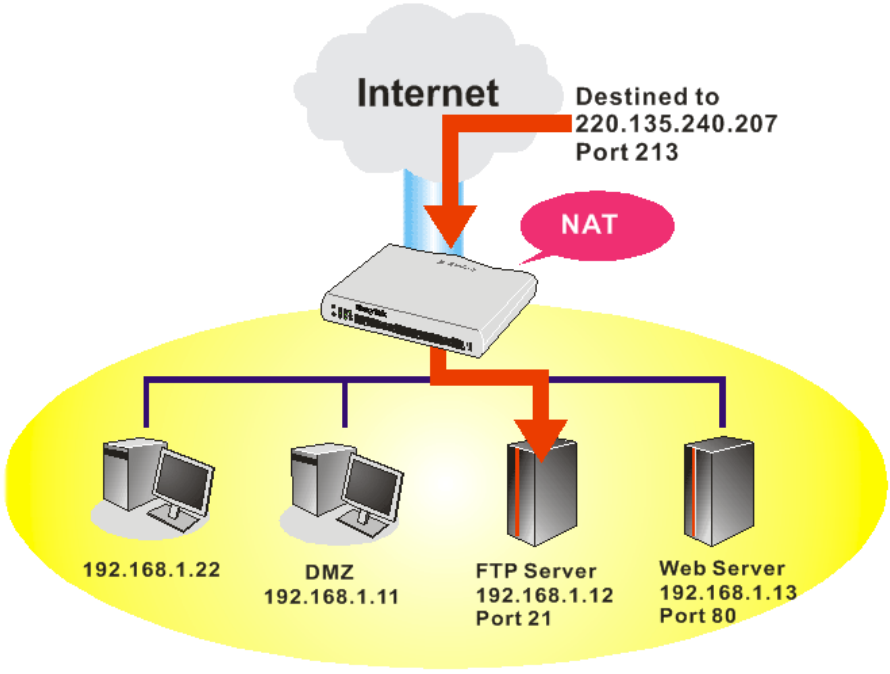
- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

Below shows the menu items for NAT.

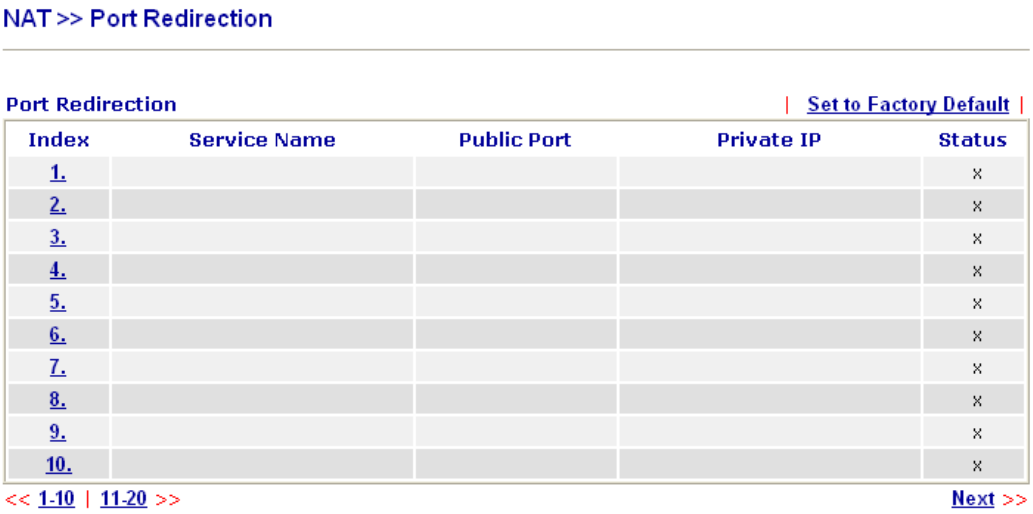
3.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.

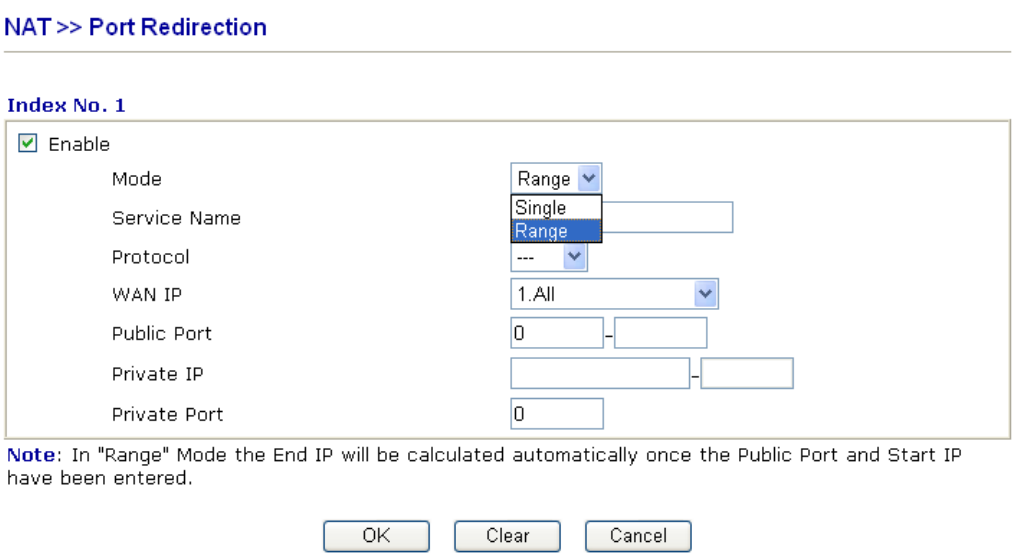


The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 20 port-mapping entries for the internal hosts.



Press any number under Index to access into next page for configuring port redirection.



Enable Check this box to enable such port redirection setting.

Mode Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.

Service Name Enter the description of the specific network service.

Protocol Select the transport layer protocol (TCP or UDP).

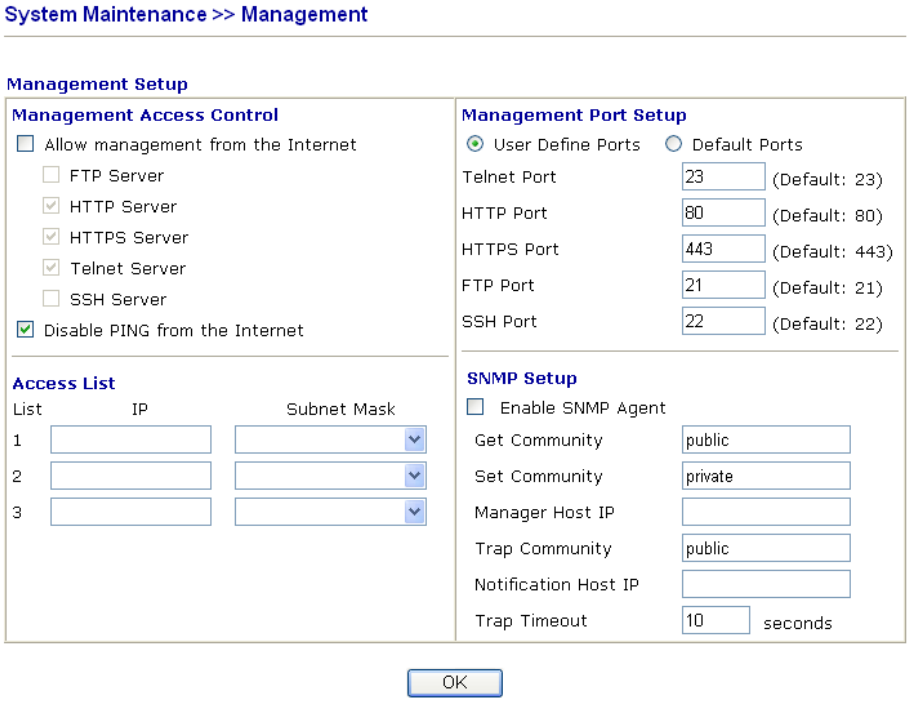
WAN IP Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to specified range of IP address and port.

Public Port Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.

Private IP	Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).
Private Port	Specify the private port number of the service offered by the internal host.
Active	Check this box to activate the port-mapping entry you have defined.

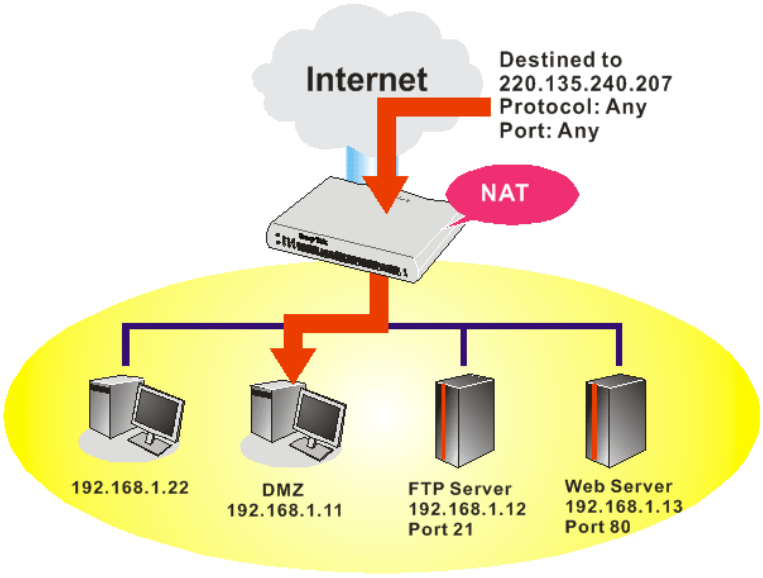
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance >>Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.



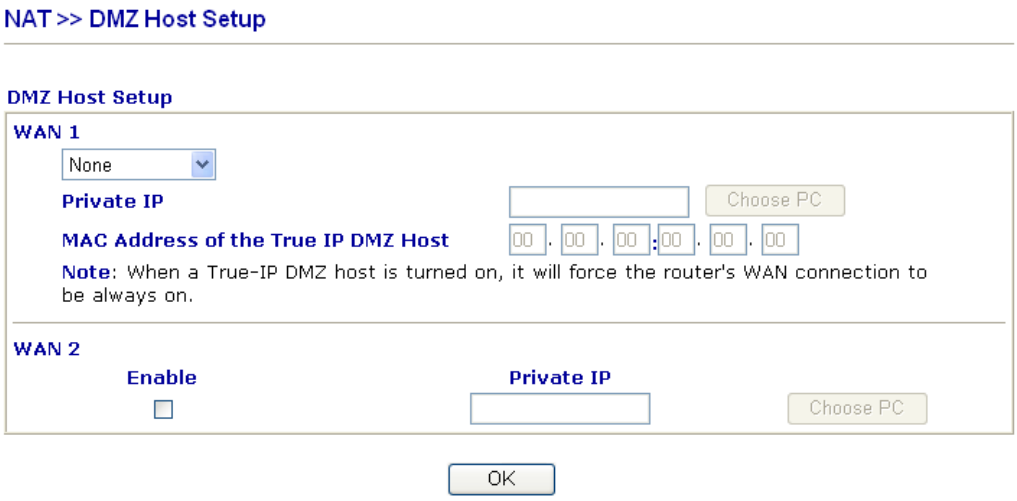
3.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.

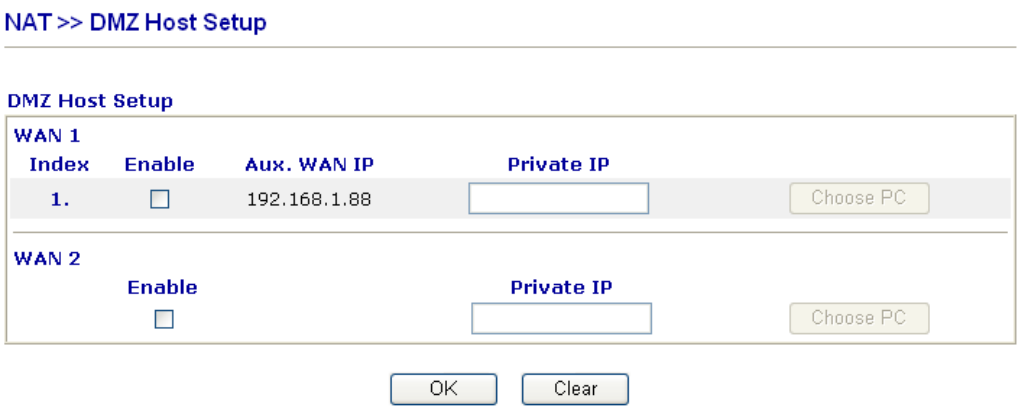


The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

Click **DMZ Host** to open the following page:


NAT >> DMZ Host Setup
DMZ Host Setup
WAN 1
None
Private IP
Choose PC
MAC Address of the True IP DMZ Host
00 . 00 . 00 : 00 . 00 . 00
Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.
WAN 2
Enable
Private IP
Choose PC
OK

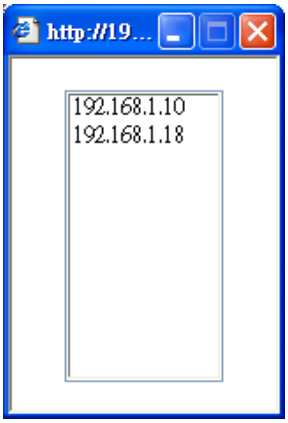
If you previously have set up **WAN Alias** for **PPPoE/PPPoA** or **MPoA** mode**,** you will find them in **Aux. WAN IP** for your selection.



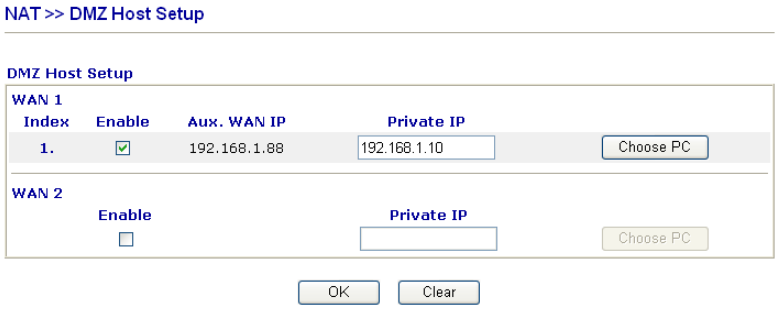
Enable Check to enable the DMZ Host function.

Private IP Enter the private IP address of the DMZ host, or click Choose PC to select one.

Choose PC Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



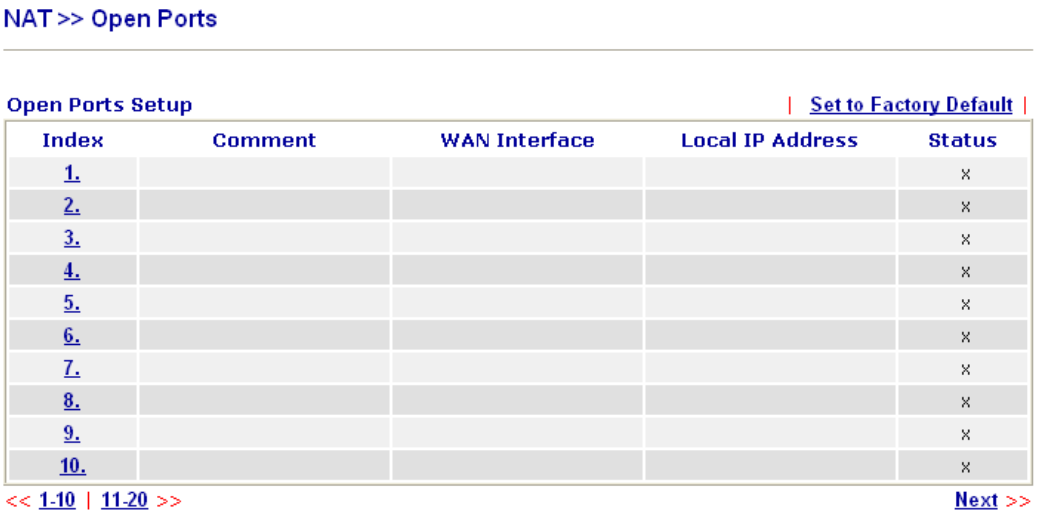
When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.



3.3.3 Open Ports

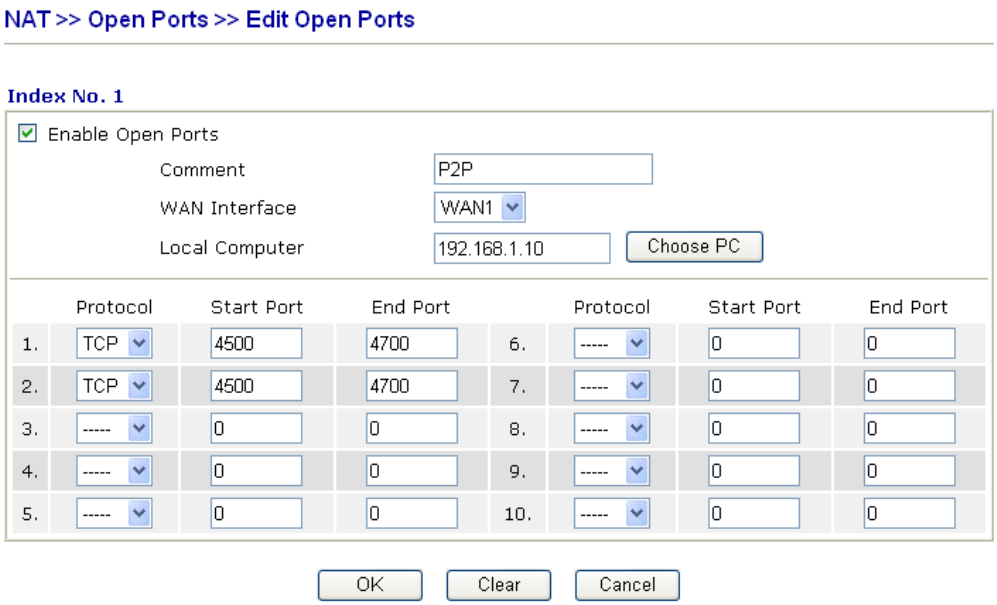
Open Ports allows you to open a range of ports for the traffic of special applications. Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

Click **Open Ports** to open the following page:



Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
WAN Interface	Display the WAN interface for the entry.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.



Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
Local Computer	Enter the private IP address of the local host or click **Choose PC** to select one.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be **TCP**, **UDP**, or **-----** (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

3.4 Firewall

3.4.1 Basics for Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

Firewall Facilities

The users on the LAN are provided with secured protection by the following firewall facilities:

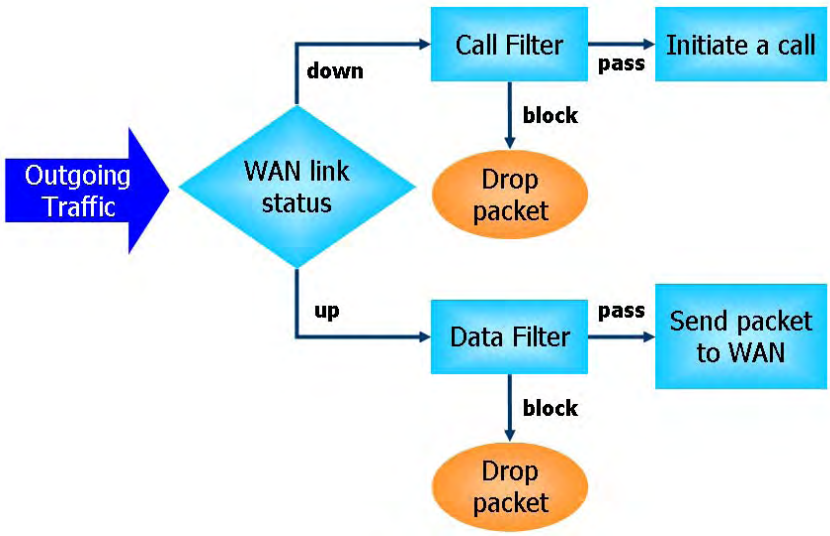
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

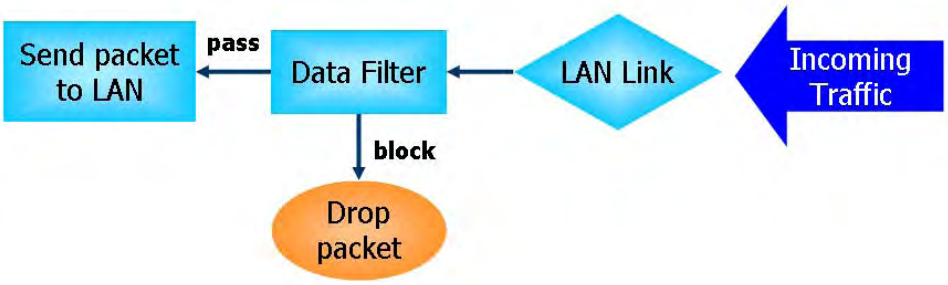
IP Filters

Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter** - When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.
- **Data Filter** - When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.





Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not just examine the header information also monitor the state of the connection.

Denial of Service (DoS) Defense

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

The below shows the attack types that DoS/DDoS defense function can detect:

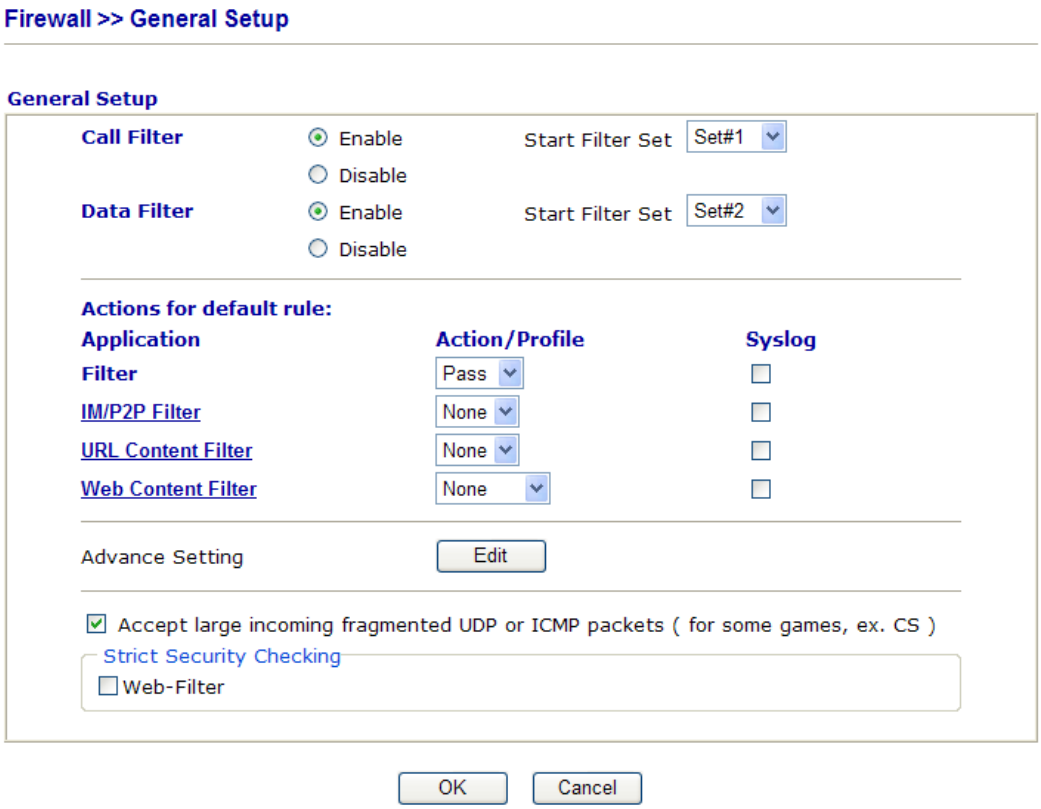
1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
9. SYN fragment
10. Fraggle attack
11. TCP flag scan
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unknown protocol

Below shows the menu items for Firewall.

3.4.2 General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, and **Accept large incoming fragmented UDP or ICMP packets**.

Click **Firewall** and click **General Setup** to open the general setup page.



Call Filter — Check **Enable** to activate the Call Filter function. Assign a start filter set for the Call Filter.

Data Filter — Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.

Action/Profile — Select **Pass** or **Block** for the packets that do not match with the filter rules.

IM/P2P Filter — Select one of the **IM/P2P Filter Profile** settings (created in **CSM>> IM/P2P Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> IM/P2P Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **IM/P2P Filter Profile** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.14.5 **Syslog/Mail Alert** for more detailed information.

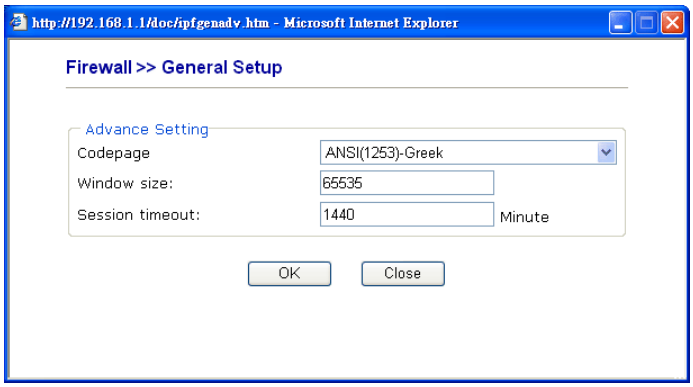
URL Content Filter — Select one of the **URL Content Filter Profile** settings (created in **CSM>> URL Content Filter Profile**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking

the Log box. It will be sent to Syslog server. Please refer to section 3.14.5 **Syslog/Mail Alert** for more detailed information.

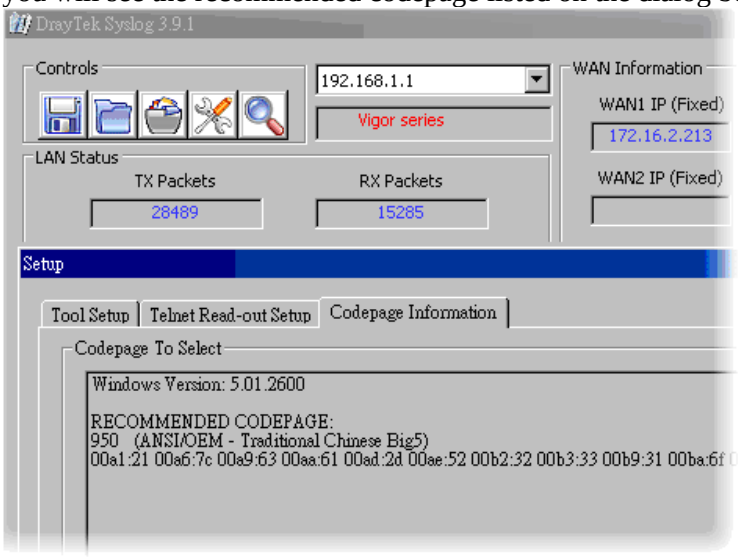
Web Content Filter Select one of the **Web Content Filter Profile** settings (created in **CSM>> Web Content Filter Profile**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter Profile** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.14.5 **Syslog/Mail Alert** for more detailed information.

Syslog For troubleshooting needs you can specify the filter log and/or CSM log here by checking the box. The log will be displayed on Draytek Syslog window.

Advance Setting Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.



Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.
If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



Window size – It determines the size of TCP protocol

(0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

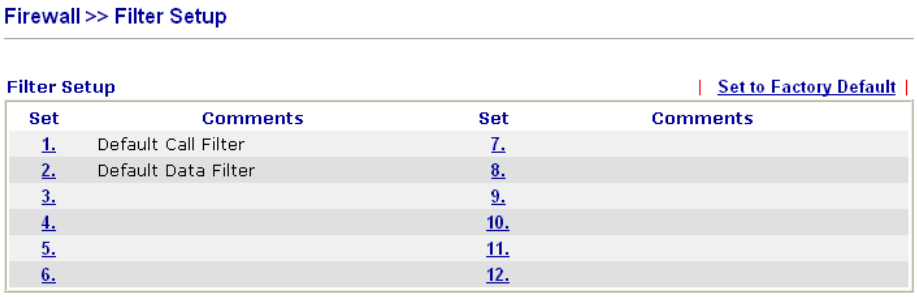
Session timeout–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

Accept large incoming.. Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "**Accept large incoming fragmented UDP or ICMP Packets**". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "**Accept large incoming fragmented UDP or ICMP Packets**".

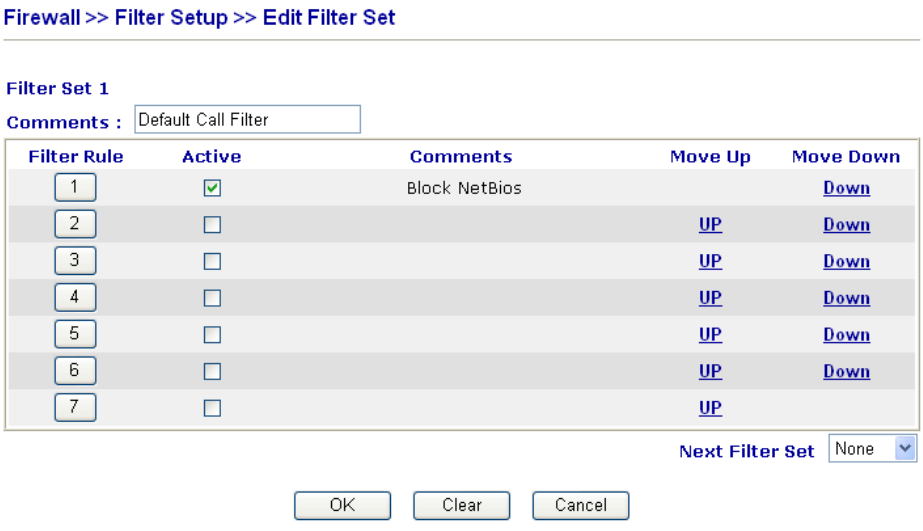
Web-Filter Check this box to promote the accuracy of web content filter. Uncheck this box to speed up the checking mechanism of web content filter.

3.4.3 Filter Setup

Click **Firewall** and click **Filter Setup** to open the setup page.

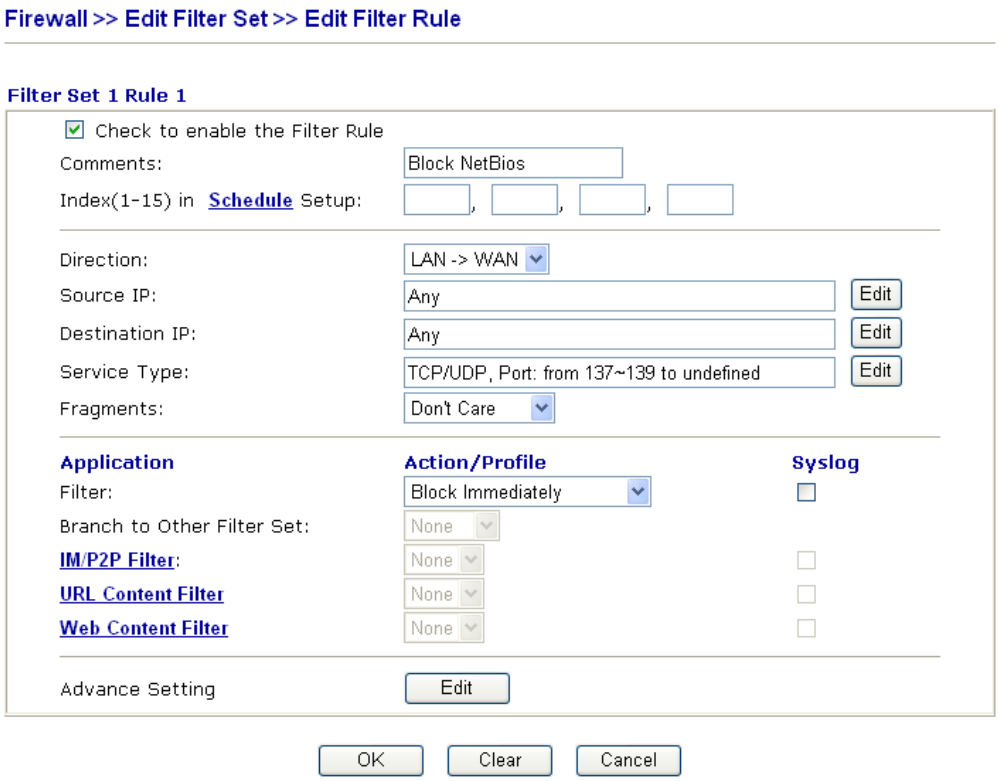


To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.

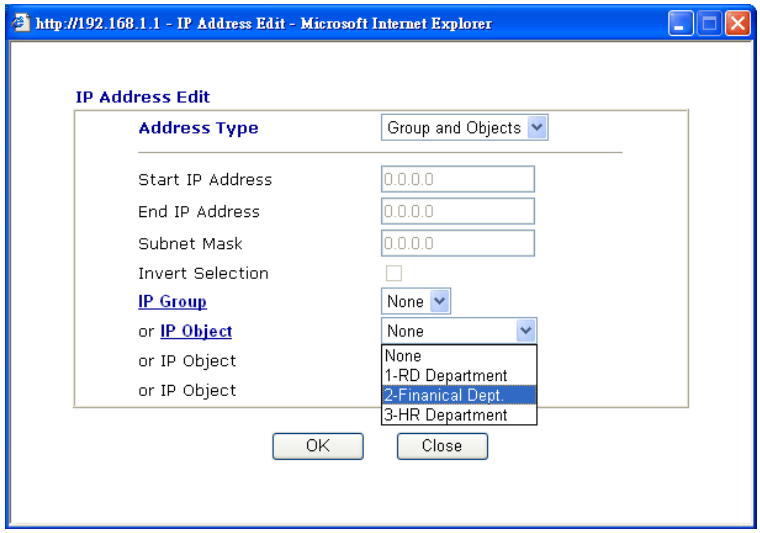


Filter Rule	Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.
Active	Enable or disable the filter rule.
Comment	Enter filter set comments/description. Maximum length is 23–character long.
Move Up/Down	Use **Up** or **Down** link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

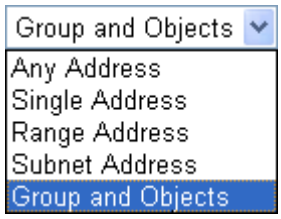
To edit **Filter Rule**, click the **Filter Rule** index button to enter the **Filter Rule** setup page.



Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14-character long.
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this filed is blank and the function will always work.
Direction	Set the direction of packet flow (LAN->WAN/WAN->LAN). It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic.
Source/Destination IP	Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.



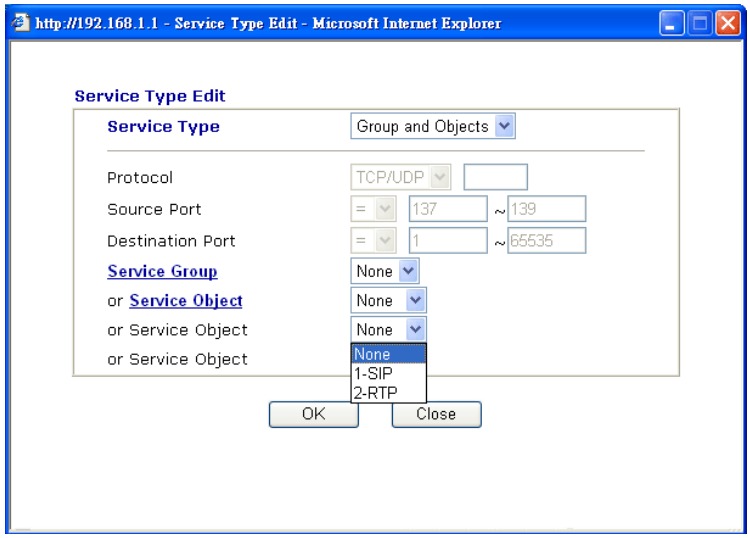
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



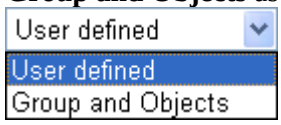
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

Service Type

Click **Edit** to access into the following dialog to choose a suitable service type.



To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you want to

	use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.  **Protocol -** Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port -** ***(=)*** – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. ***(!=)*** – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. ***(>)*** – the port number greater than this value is available. ***(<)*** – the port number less than this value is available for this profile. **Service Group/Object -** Use the drop down list to choose the one that you want.
Fragments	Specify the action for fragmented packets. And it is used for **Data Filter** only. ***Don't care -***No action will be taken towards fragmented packets. ***Unfragmented -***Apply the rule to unfragmented packets. ***Fragmented -*** Apply the rule to fragmented packets. ***Too Short -*** Apply the rule only to packets that are too short to contain a complete header.
Filter	Specifies the action to be taken when packets match the rule. **Block Immediately -** Packets matching the rule will be dropped immediately. **Pass Immediately -** Packets matching the rule will be passed immediately. **Block If No Further Match -** A packet matching the rule, and that does not match further rules, will be dropped. **Pass If No Further Match -** A packet matching the rule, and that does not match further rules, will be passed through.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
IM/P2P Filter	Select one of the **IM/P2P Filter Profile** settings (created in **CSM>> IM/P2P Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> IM/P2P Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **IM/P2P Filter Profile** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.14.5 **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It

will be sent to Syslog server. Please refer to section 3.14.5 **Syslog/Mail Alert** for more detailed information.

Web Content Filter

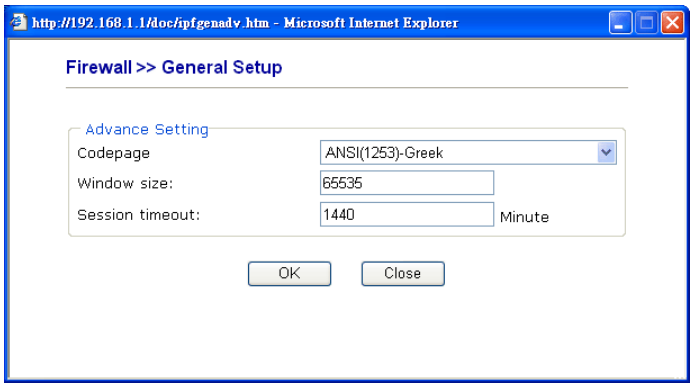
Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.14.5 **Syslog/Mail Alert** for more detailed information.

SysLog

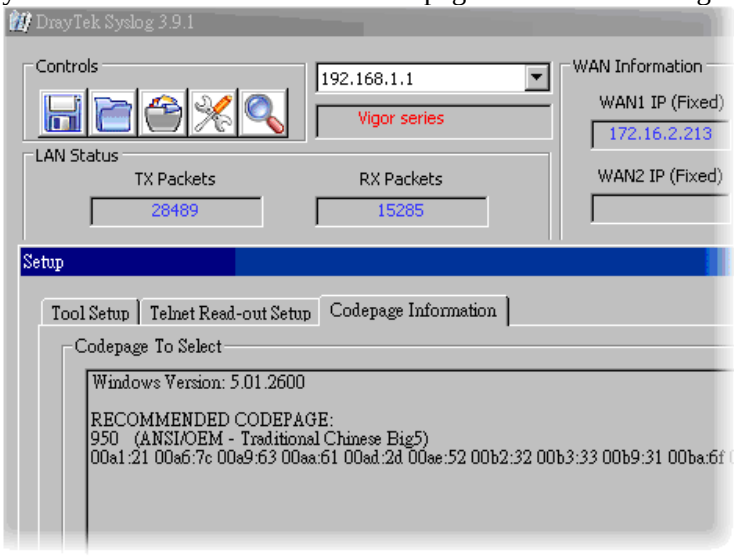
For troubleshooting needs you can specify the filter log and/or CSM log here. Check the corresponding box to enable the log function. Then, the filter log and/or CSM log will be shown on Draytek Syslog window.

Advance Setting

Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.



Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.
If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

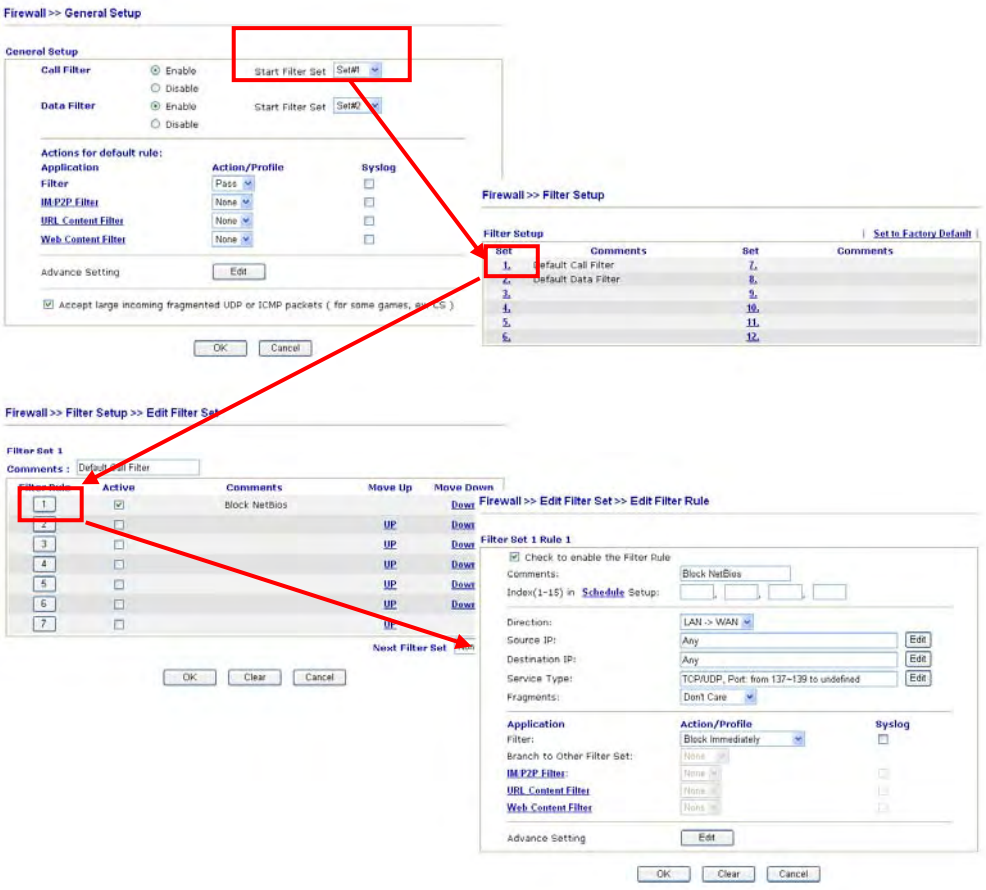


Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

Session timeout–Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.

Example

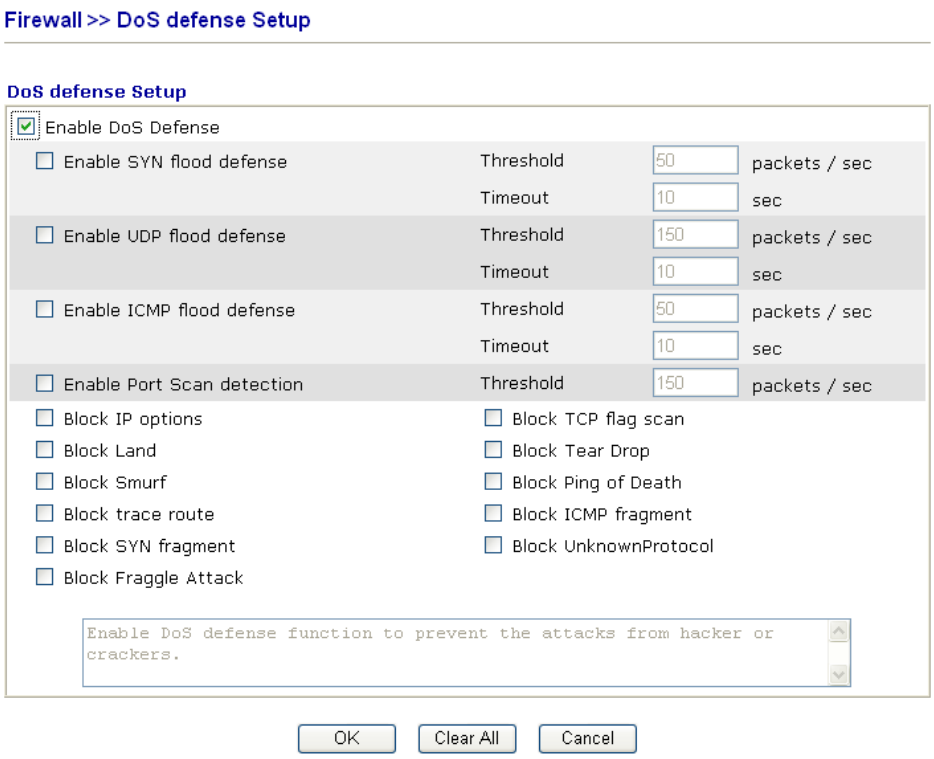
As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.



3.4.4 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the **DoS Defense** setup. The DoS Defense functionality is disabled for default.

Click **Firewall** and click **DoS Defense** to open the setup page.



Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever

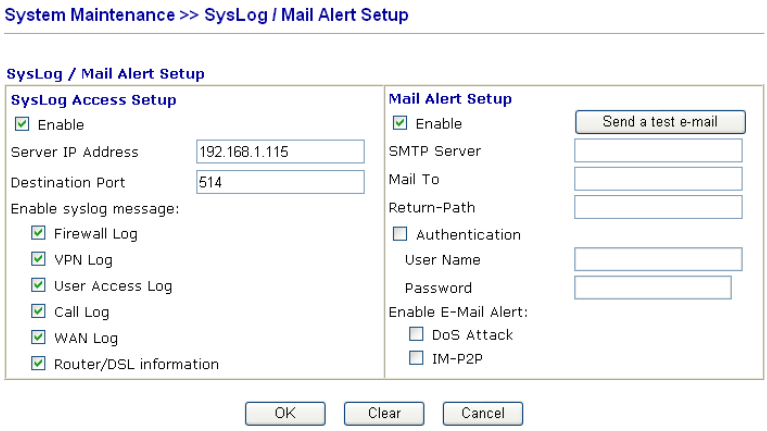
	detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unknown Protocol	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to

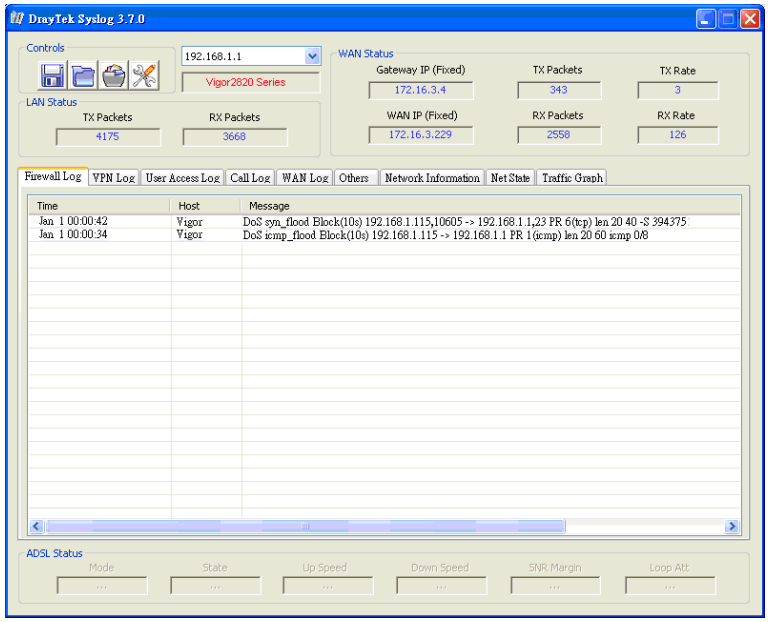
indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.

Warning Messages

We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.

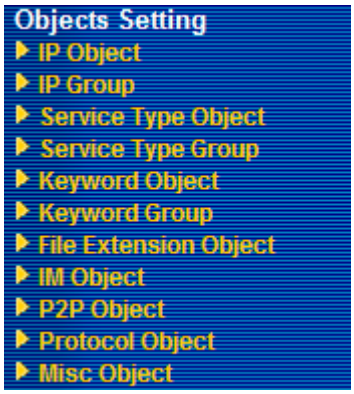
All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.





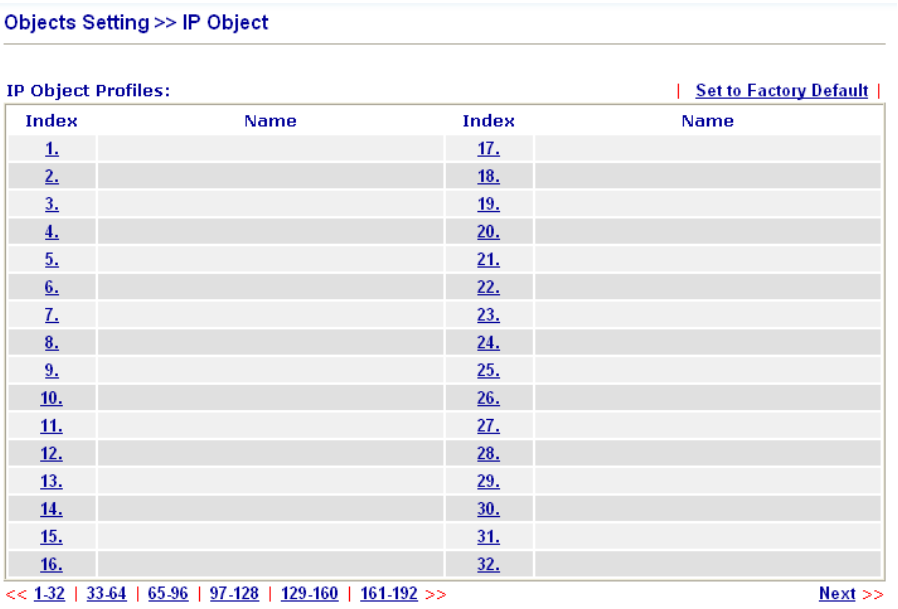
3.5 Objects Setting

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with ***objects*** and bind them with ***groups*** for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).



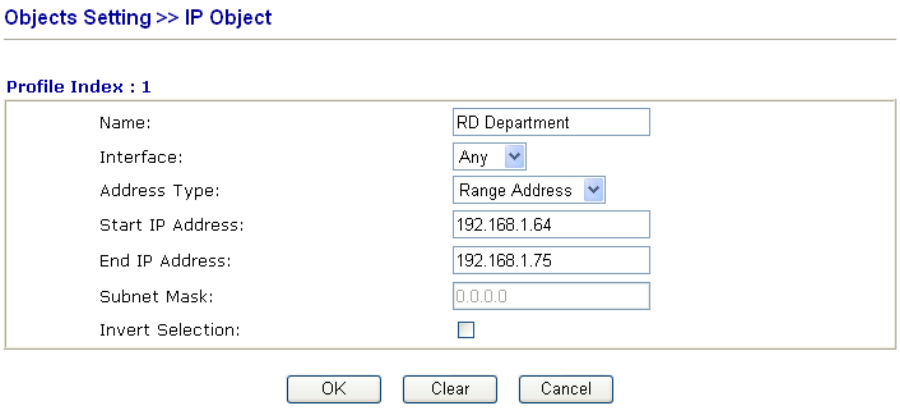
3.5.1 IP Object

You can set up to 192 sets of IP Objects with different conditions.



Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Name Type a name for this profile. Maximum 15 characters are allowed.

Interface Choose a proper interface (WAN, LAN or Any).

For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the **Interface** here, and choose LAN as the direction setting in **Edit Filter Rule**, then all the IP addresses specified with LAN interface will be opened for you to choose in **Edit Filter Rule** page.

Address Type Determine the address type for the IP address.
Select **Single Address** if this object contains one IP address only.
Select **Range Address** if this object contains several IPs within a range.
Select **Subnet Address** if this object contains one subnet for IP address.
Select **Any Address** if this object contains any IP address.

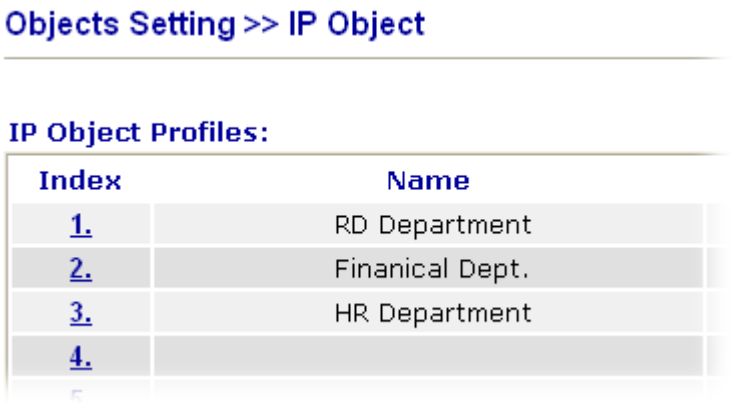
Start IP Address Type the start IP address for Single Address type.

End IP Address Type the end IP address if the Range Address type is selected.

Subnet Mask Type the subnet mask if the Subnet Address type is selected.

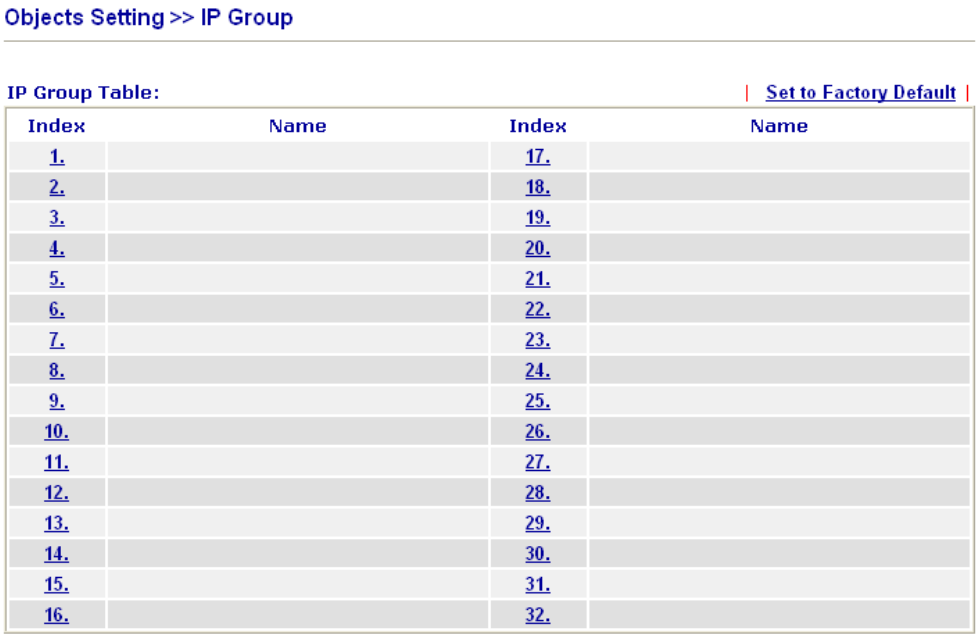
Invert Selection If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

Below is an example of IP objects settings.



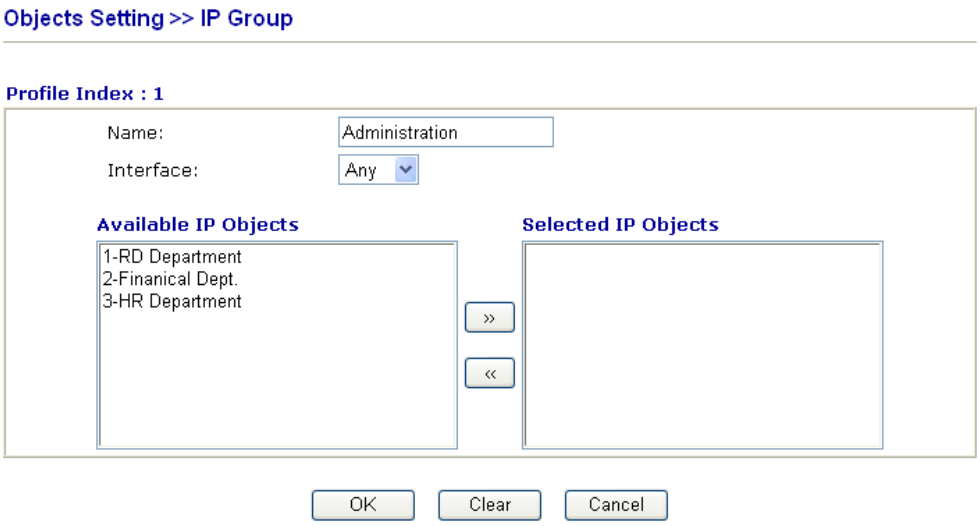
3.5.2 IP Group

This page allows you to bind several IP objects into one IP group.



Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Name Type a name for this profile. Maximum 15 characters are allowed.

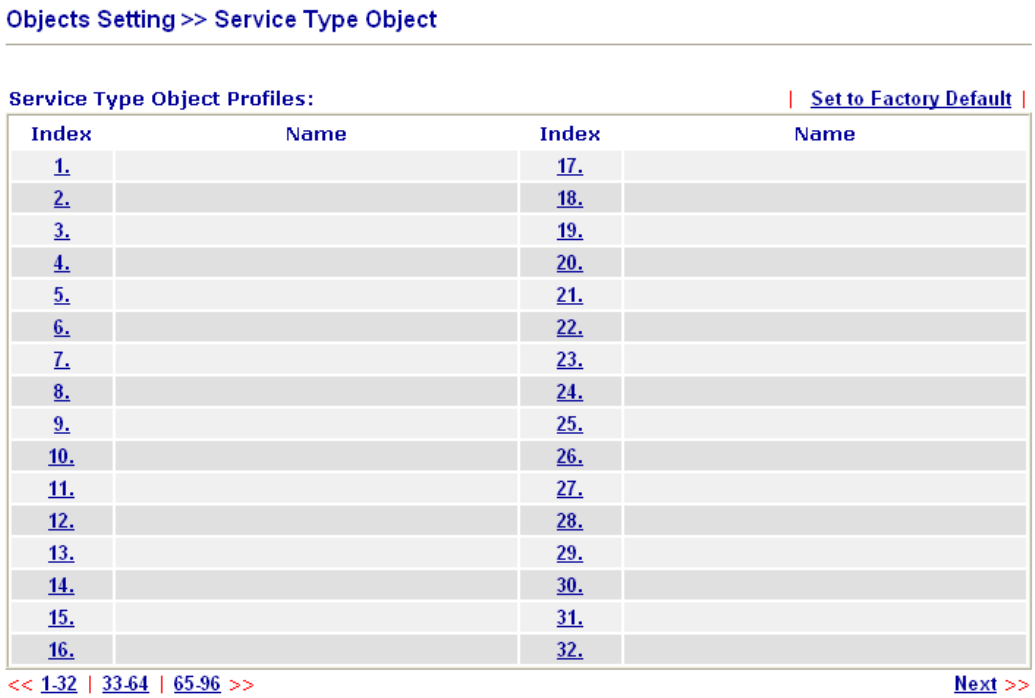
Interface Choose WAN, LAN or Any to display all the available IP objects with the specified interface.

Available IP Objects All the available IP objects with the specified interface chosen above will be shown in this box.

Selected IP Objects Click >> button to add the selected IP objects in this box.

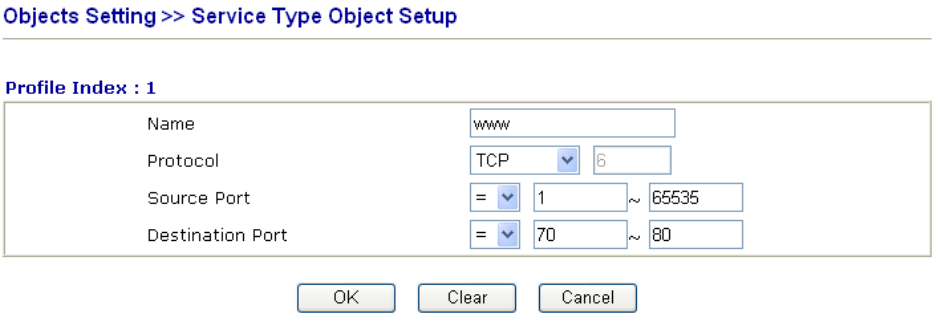
3.5.3 Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.



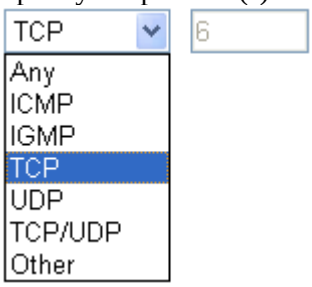
Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Name Type a name for this profile.

Protocol Specify the protocol(s) which this profile will apply to.



Source/Destination Port **Source Port** and the **Destination Port** column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.

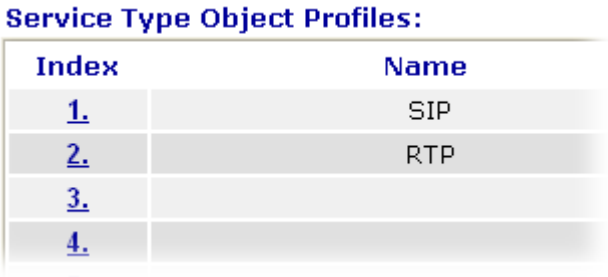
(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.

(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

(>) – the port number greater than this value is available.

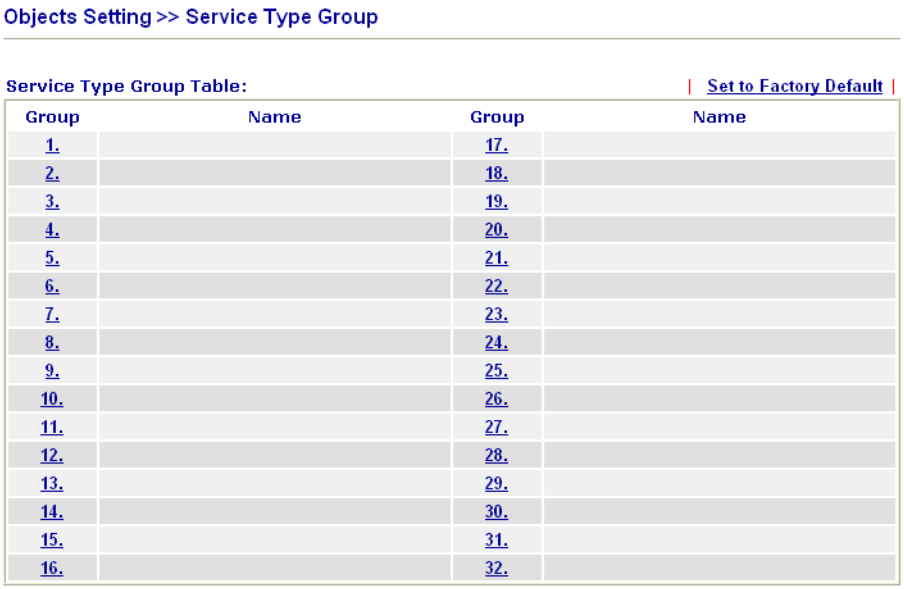
(<) – the port number less than this value is available for this profile.

Below is an example of service type objects settings.



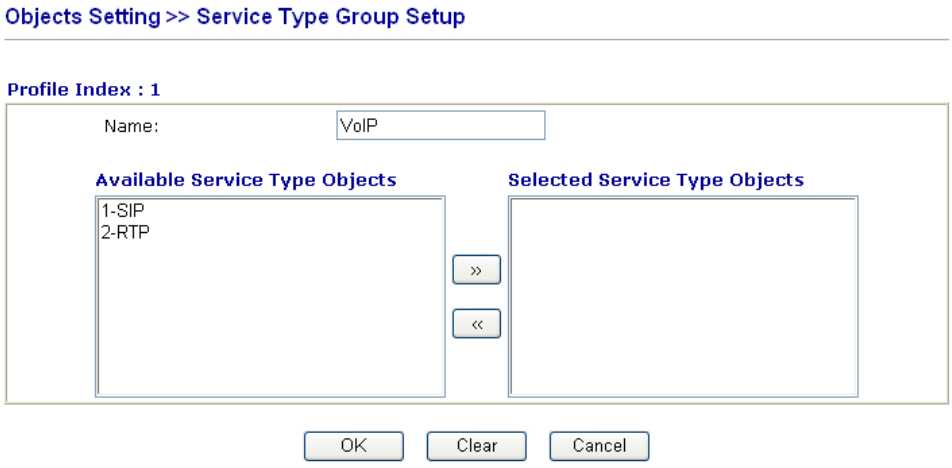
3.5.4 Service Type Group

This page allows you to bind several service types into one group.



Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



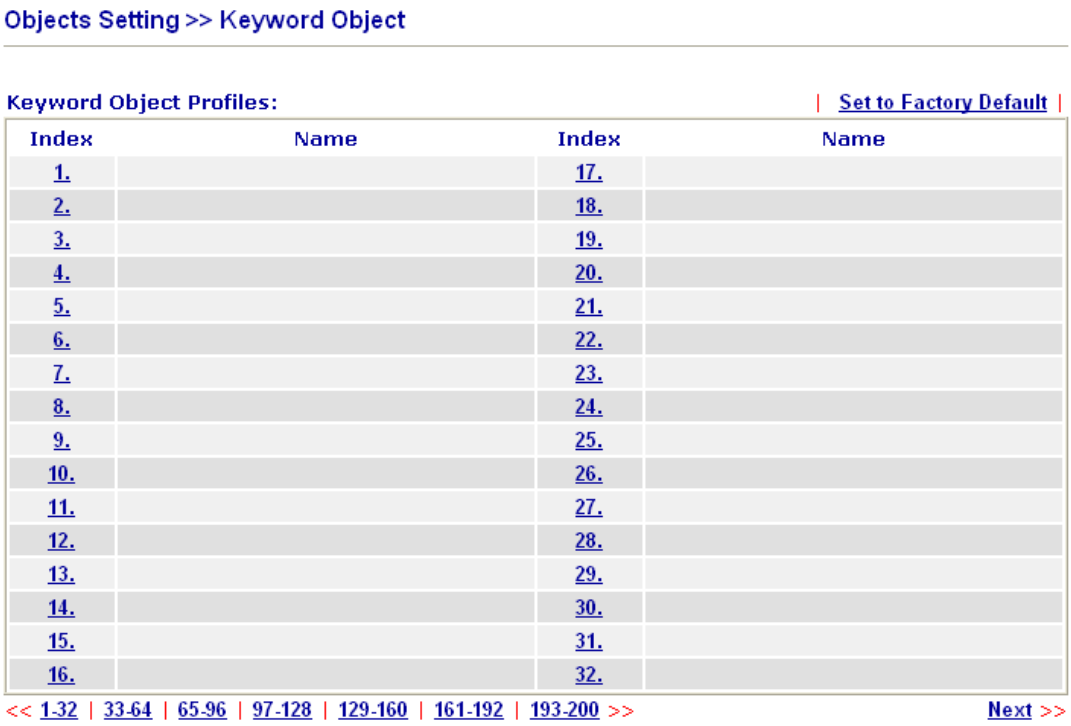
Name Type a name for this profile.

Available Service Type Objects All the available service objects that you have added on **Objects Setting>>Service Type Object** will be shown in this box.

Selected Service Type Objects Click >> button to add the selected IP objects in this box.

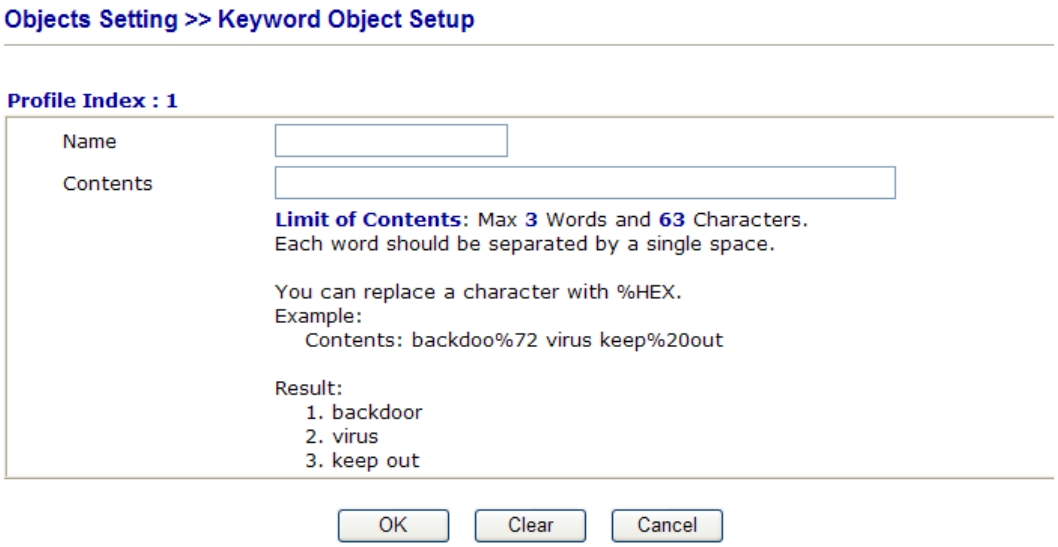
3.5.5 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in **CSM >>URL Web Content Filter Profile.**



Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.

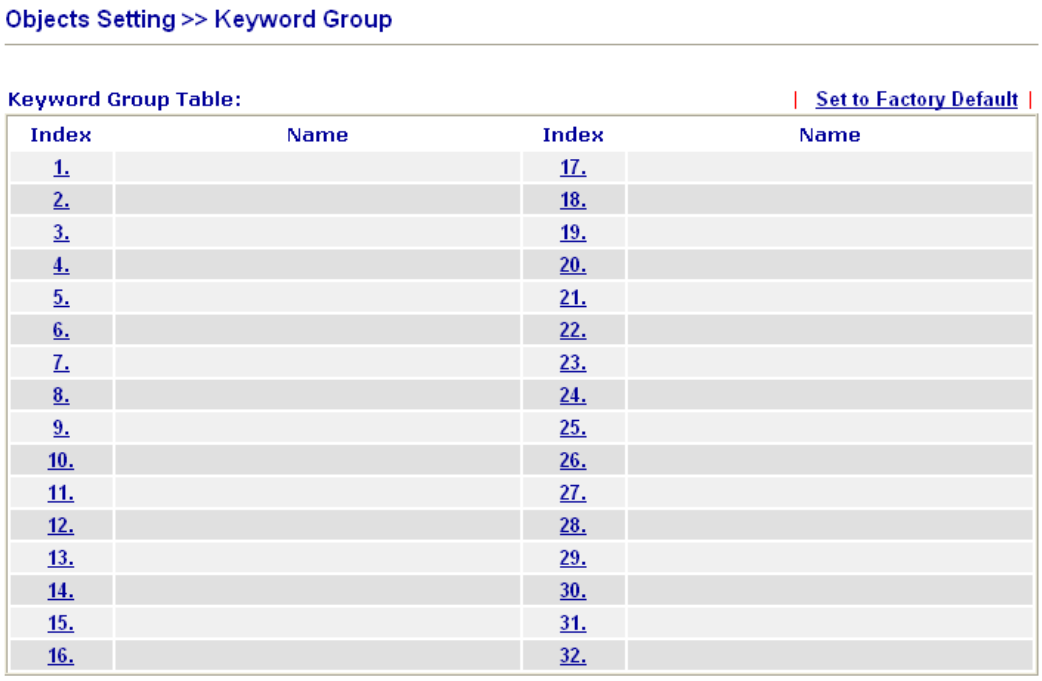


Name Type a name for this profile, e.g., game.

Contents Type the content for such profile. For example, type *gambling* as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

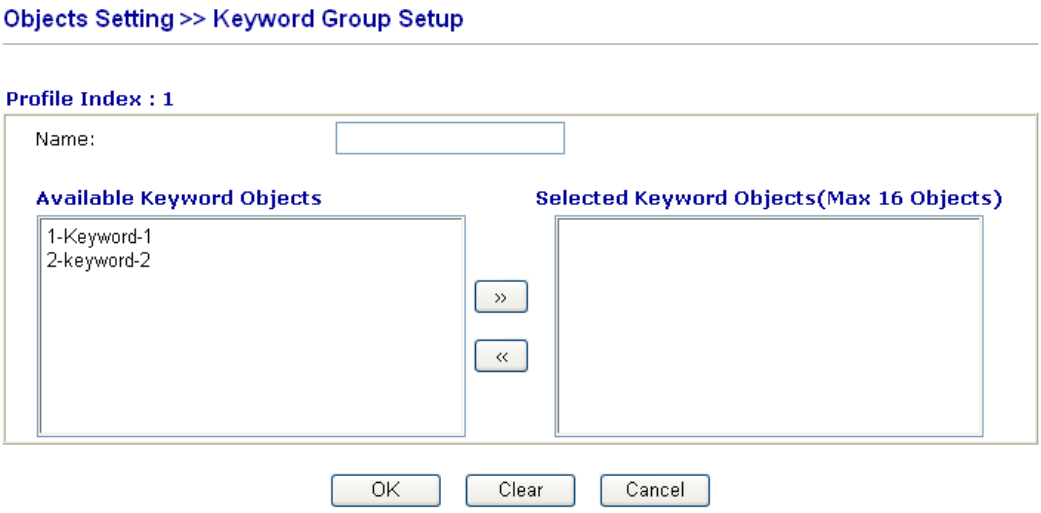
3.5.6 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in **CSM >>URL Web Content Filter Profile**.



Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.



Name Type a name for this group.

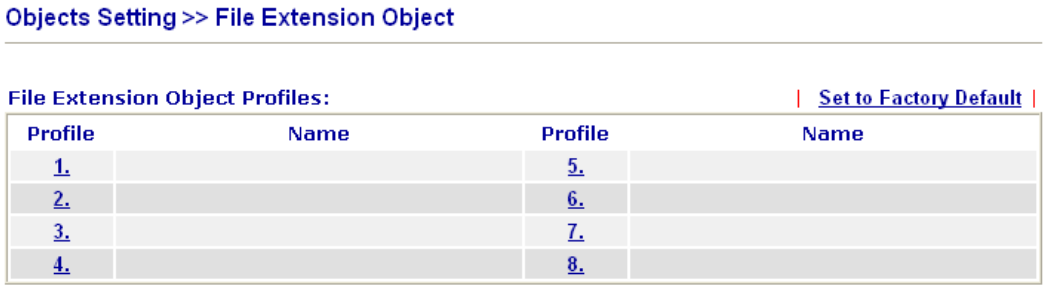
Available Keyword Objects You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.

Selected Keyword Objects Click >> button to add the selected Keyword objects in this box.

3.5.7 File Extension Object

This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

Profile 1 with name of "default" is the default profile, some files with the file extensions specified in this profile will be ignored and not be scanned by Vigor router.



Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details.

Profile Name Type a name for this profile.

Type a name for such profile and check all the items of file extension that will be processed in the router. Finally, click **OK** to save this profile.

3.5.8 IM Object

This page allows you to set 32 profiles for Instant Messenger. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.

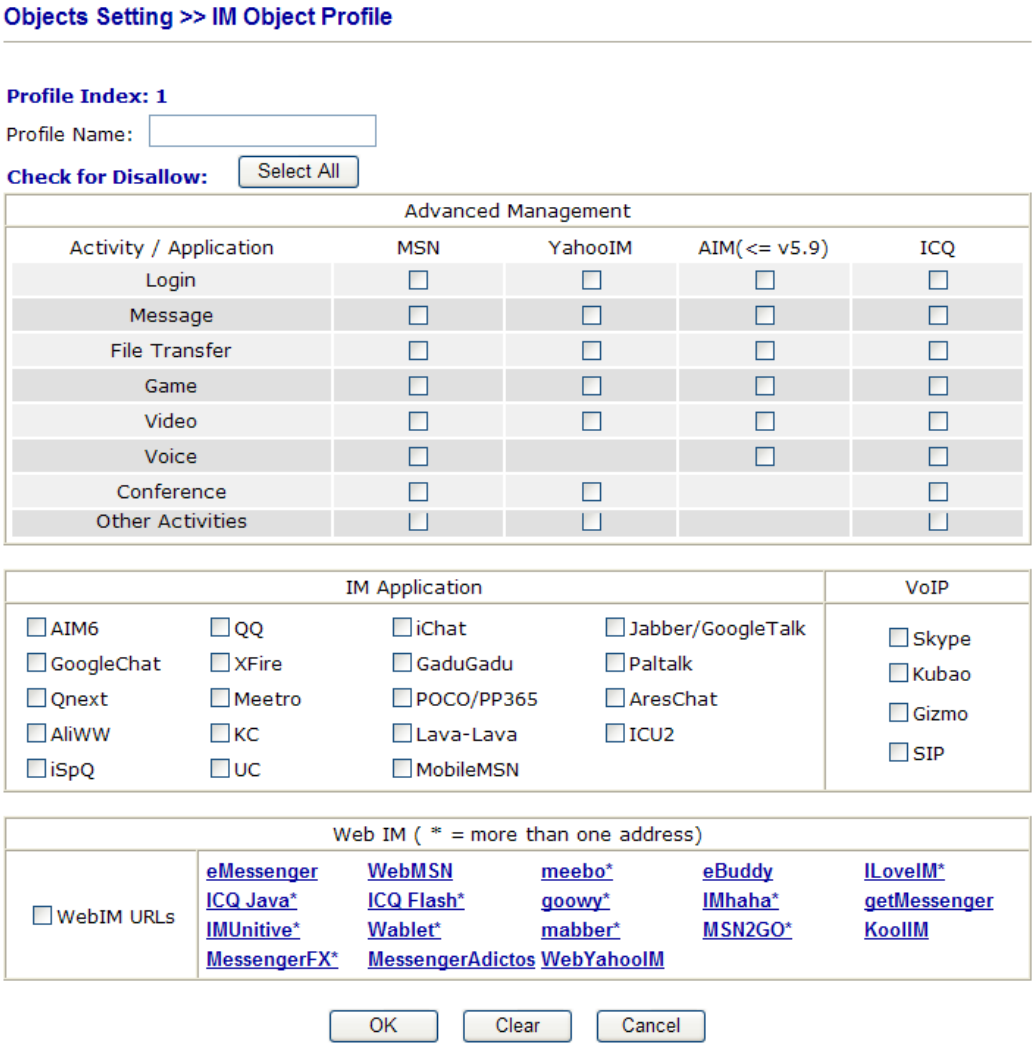
Objects Setting >> IM Object Profile

IM Profile Table: | Set to Factory Default |

Profile	Name	Profile	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. There are several types of Instant Messenger (IM) provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **IM Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

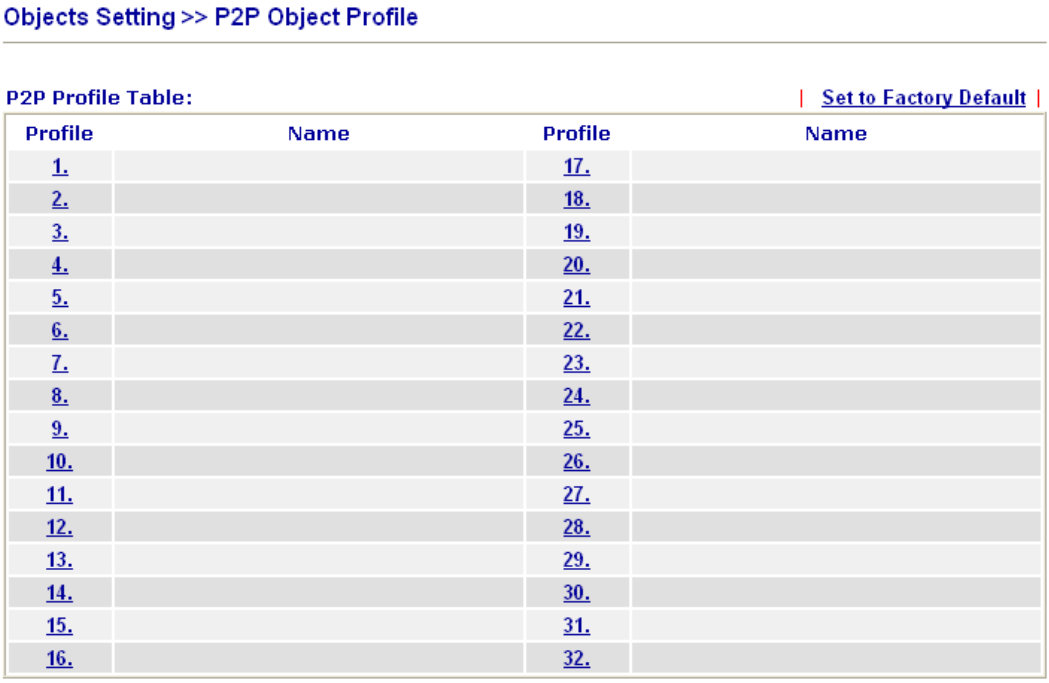


Profile Name Type a name for this profile.

Type a name for such profile and check all the items that not allowed to be used in the host. Finally, click **OK** to save this profile.

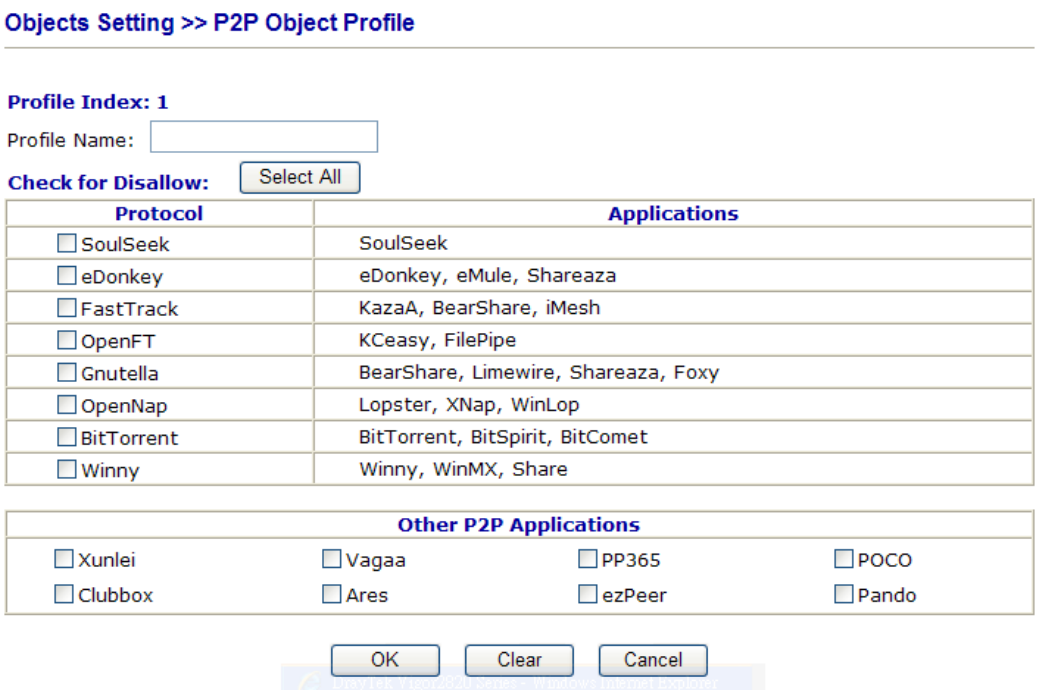
3.5.9 P2P Object

This page allows you to set 32 profiles for peer-to-peer application. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.



Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. There are several items for P2P protocols provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **P2P Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

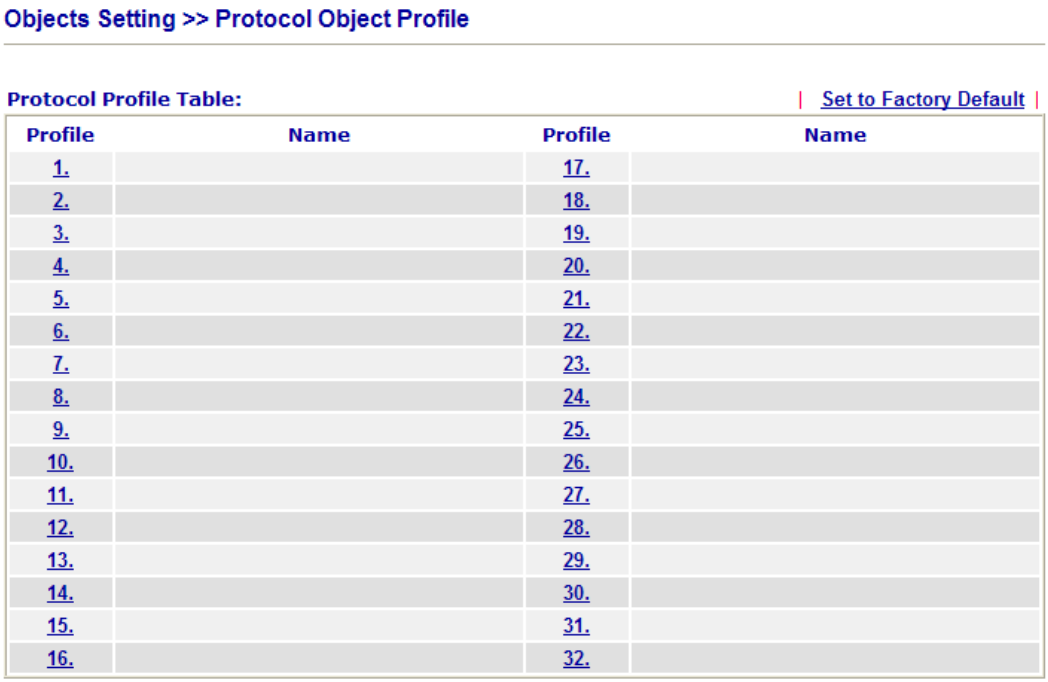


Profile Name Type a name for this profile.

Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.

3.5.10 Protocol Object

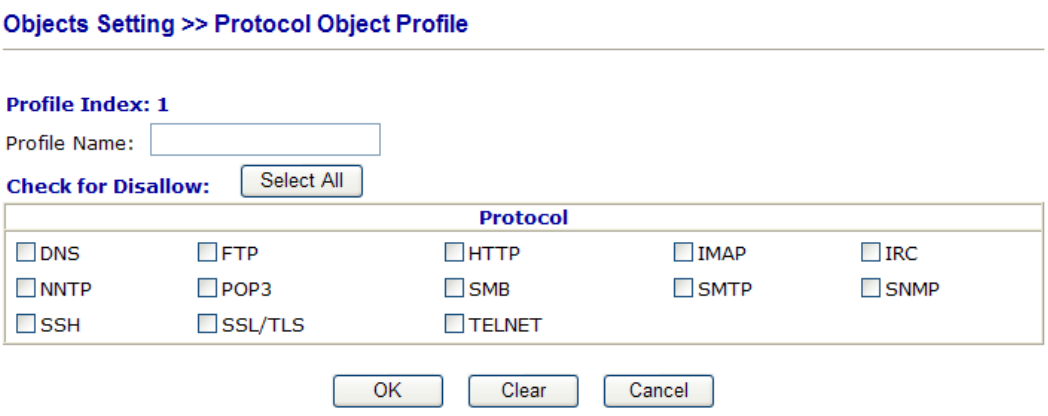
This page allows you to set 32 profiles for applications in protocol communication. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.



Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. Internet protocols are listed in the page for you to choose to disallow people using. Any computer controlled or passed through the router will be restricted by this profile if it tries to use the protocol to communicate with others.

Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **Protocol Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

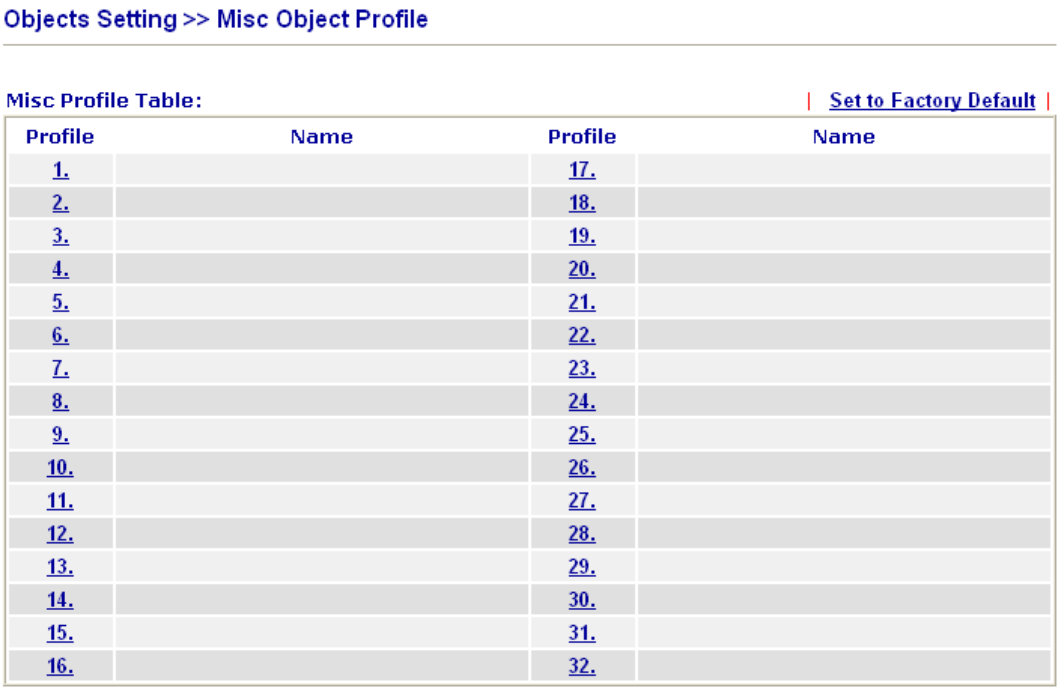


Profile Name Type a name for this profile.

Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.

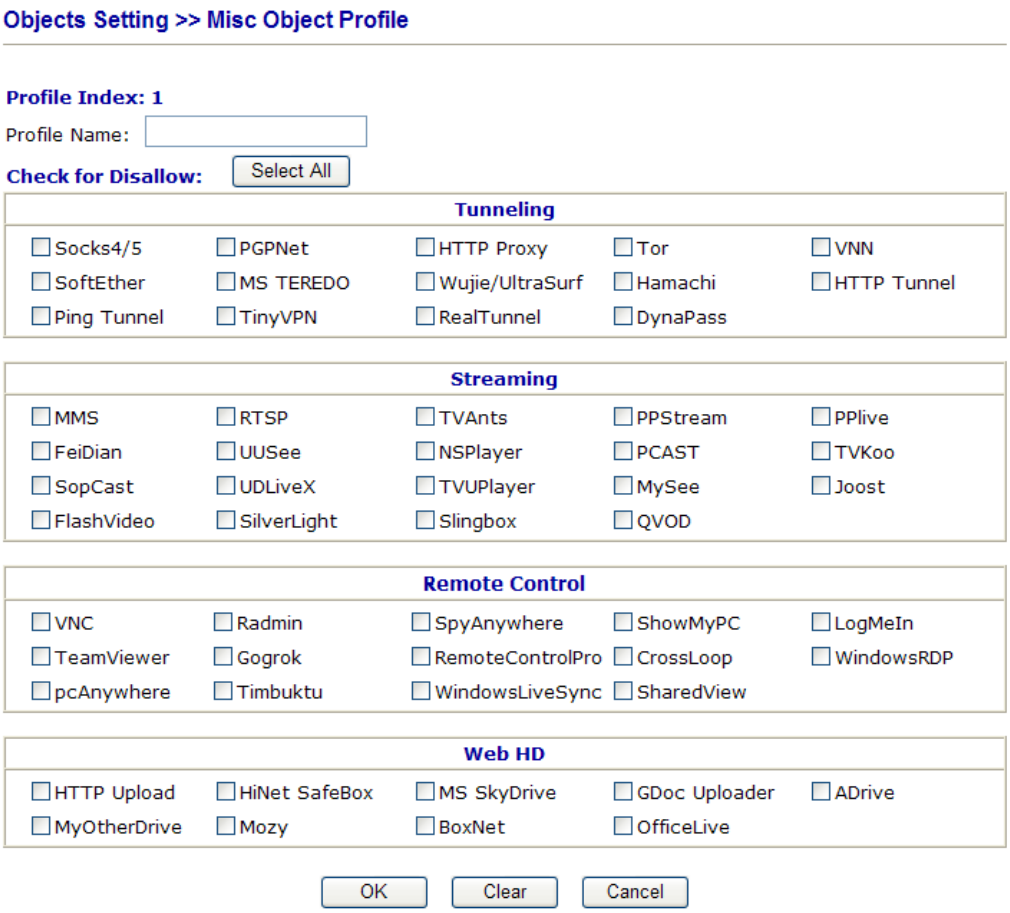
3.5.11 Misc Object

This page allows you to set 32 profiles for miscellaneous applications. These profiles will be applied in **CSM>>IM/P2P Filter Profile** for filtering.



Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. Applications for tunneling and streaming are listed in the page for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **Misc Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.



Profile Name Type a name for this profile.

Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.

3.6 CSM

CSM is an abbreviation of **Content Security Management** which is used to control IM/P2P usage, filter the web content and URL content to reach a goal of security management.

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

IM/P2P Filter

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Web Content Filter

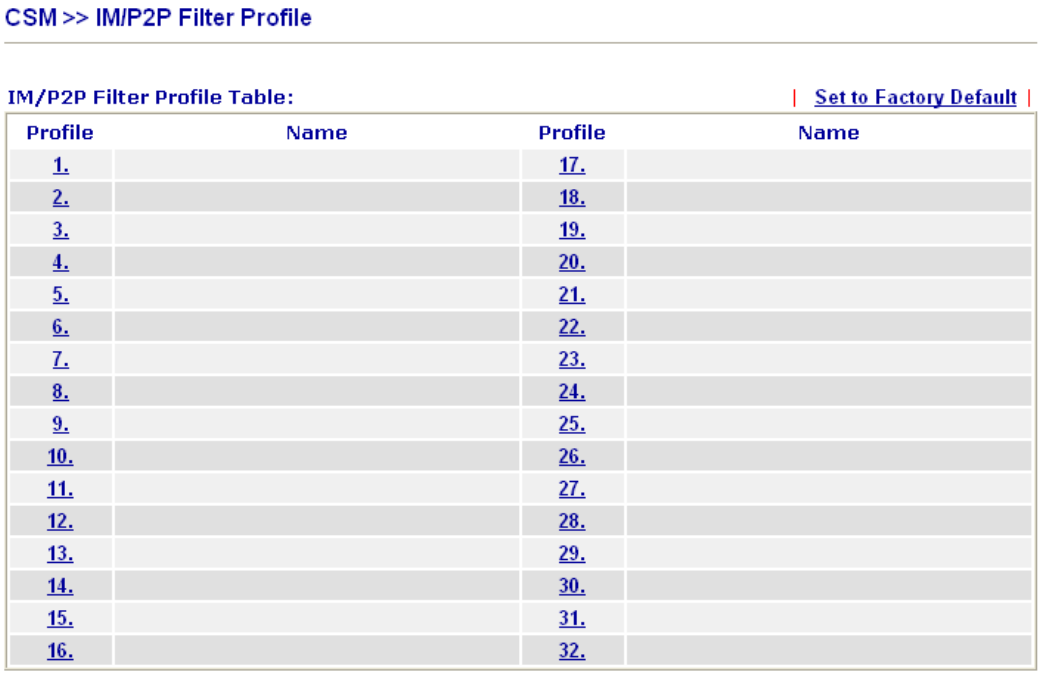
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Note: The priority of URL Content Filter is higher than Web Content Filter.

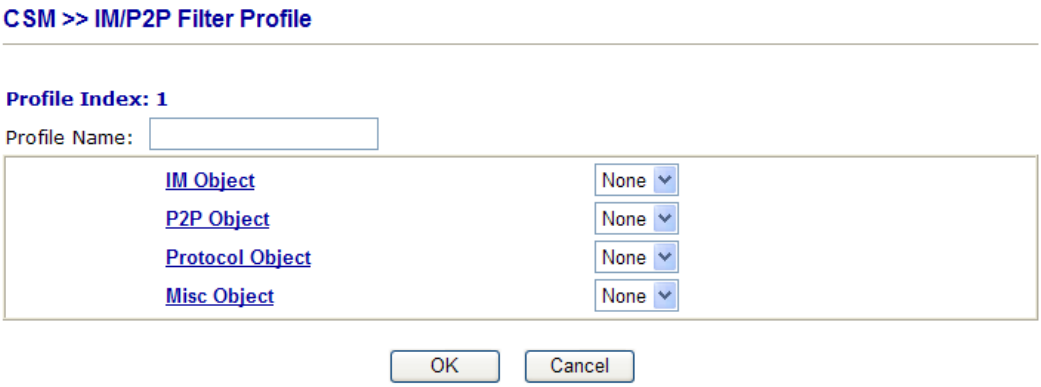
3.6.1 IM/P2P Filter Profile

You can define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application. Such profile will be used in **Firewall>>General Setup** and **Firewall>>Filter Setup** pages.



Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Profile Name Type a name for the CSM profile.

Each profile can contain three objects settings, IM Object, P2P Object, Protocol Object and Misc Object. Such profile can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

3.6.2 URL Content Filter

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

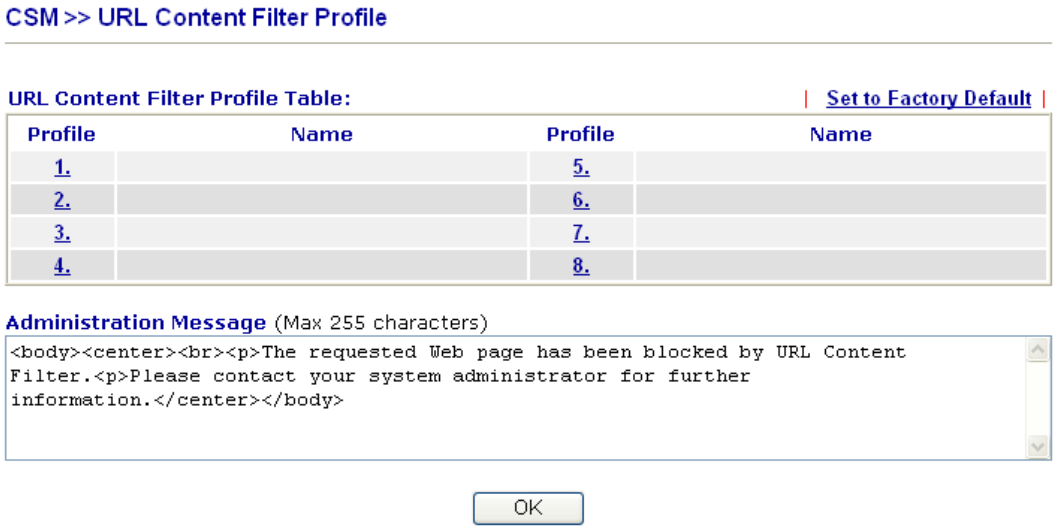
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

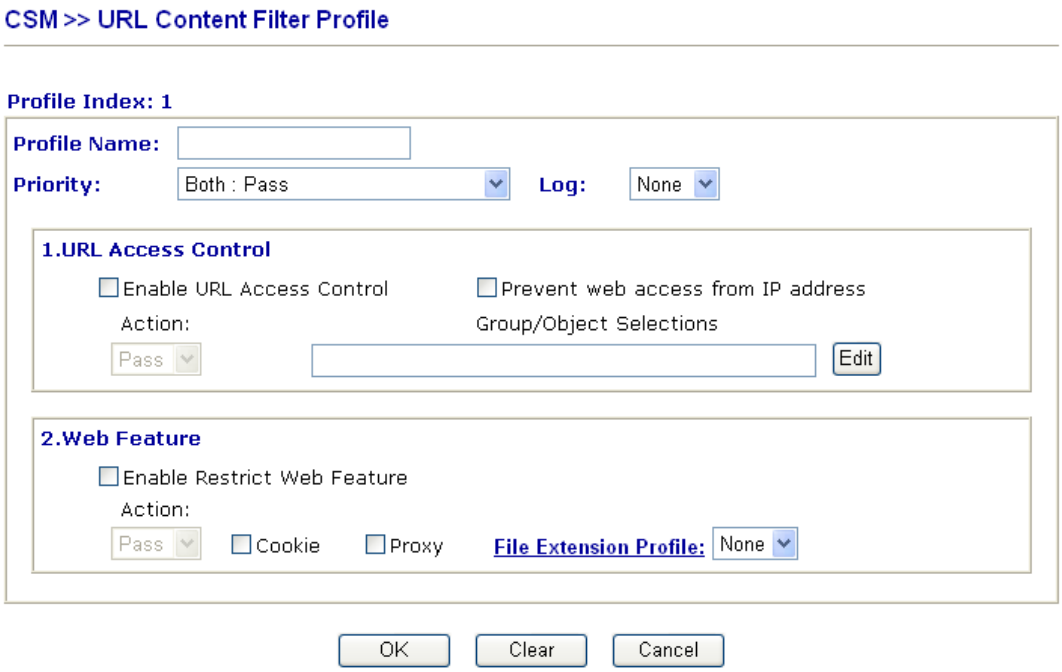
For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click **CSM** and click **URL Content Filter Profile** to open the profile setting page.

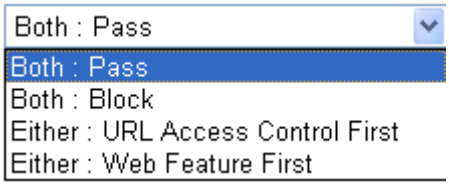


You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.



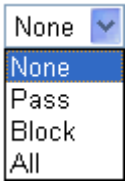
Profile Name Type the name for such profile.

Priority It determines the action that this router will apply.
Both: Pass – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.
Both: Block –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.
Either: URL Access Control First – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.
Either: Web Feature First –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.



Log **None** – There is no log file will be recorded for this profile.
Pass – Only the log about Pass will be recorded in Syslog.
Block – Only the log about Block will be recorded in Syslog.

All – All the actions (Pass and Block) will be recorded in Syslog.



URL Access Control

Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for **URL Access Control** is higher than **Restrict Web Feature**. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.

Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

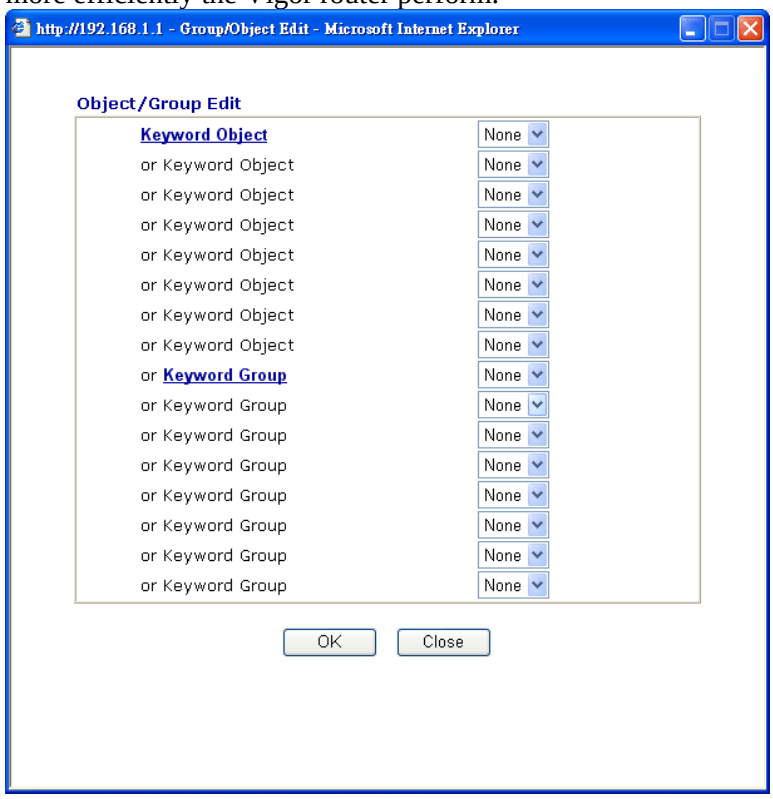
Action – This setting is available only when **Either : URL Access Control First** or **Either : Web Feature First** is selected. ***Pass*** - Allow accessing into the corresponding webpage with the keywords listed on the box below.

Block **-** Restrict accessing into the corresponding webpage with the keywords listed on the box below.

If the web pages do not match with the keyword set here, it will be processed with reverse action.

Group/Object Selections – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the

more efficiently the Vigor router perform.



Web Feature

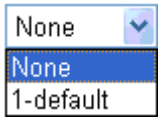
Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.

Action - This setting is available only when **Either : URL Access Control First** or **Either : Web Feature Firs** is selected. **Pass** allows accessing into the corresponding webpage with the keywords listed on the box below.
***Pass* -** Allow accessing into the corresponding webpage with the keywords listed on the box below.
***Block* -** Restrict accessing into the corresponding webpage with the keywords listed on the box below.
If the web pages do not match with the specified feature set here, it will be processed with reverse action.

Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.

Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages.

File Extension Profile – Choose one of the profiles that you configured in **Object Setting>> File Extension Objects** previously for passing or blocking the file downloading.



3.6.3 Web Content Filter

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

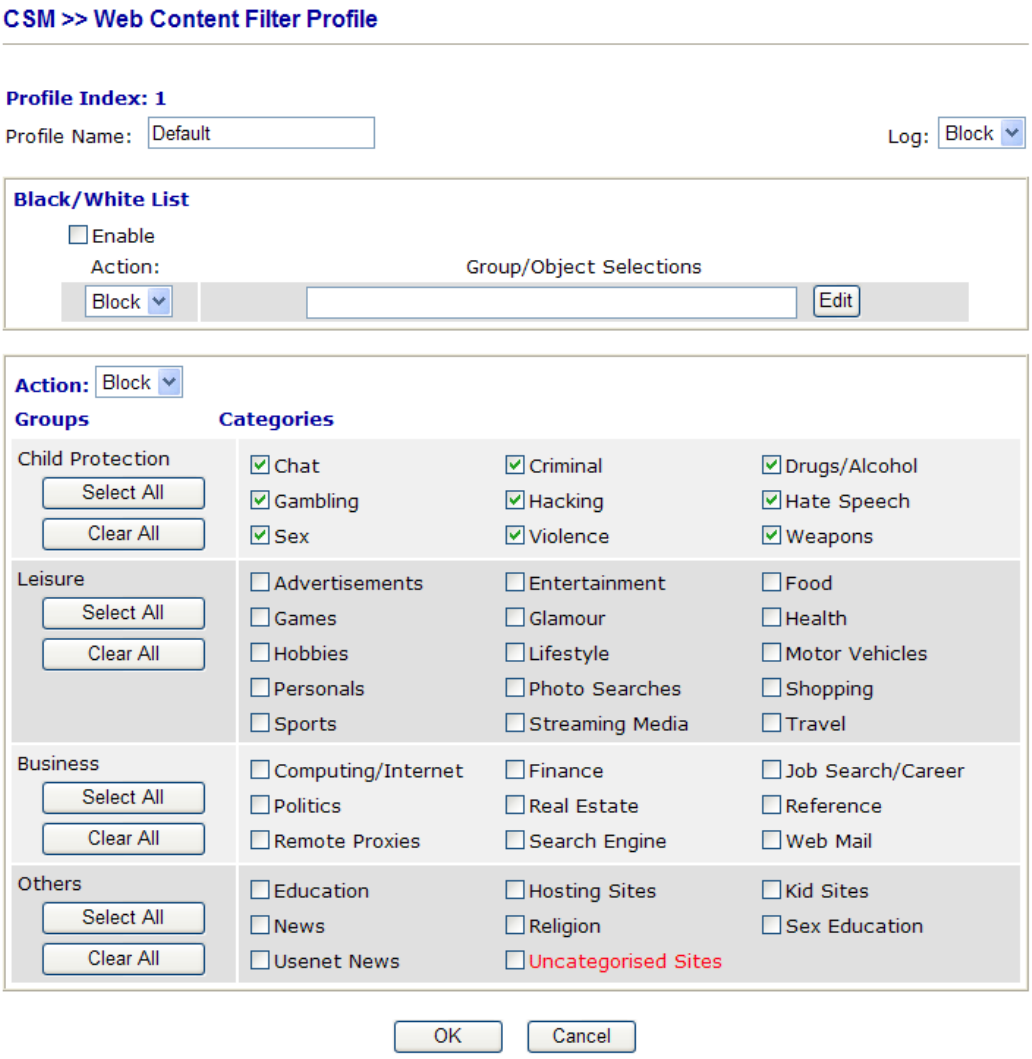
Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page.

Setup Query Server It is recommend for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.

Setup Test Server It is recommend for you to use the default setting, auto-selected. By the way, you can click the link of **Test a site to verify whether it is categorized** to access into the test server selected.

You can set eight profiles as Web content filter. Simply click the index number under Profile to open the following web page.



Black/White List

Enable – Check this box to enable the filtering mechanism with the condition of black/white list. Click **Edit** to open the keyword object /group selection window and choose the one you want to use. Then, choose the action for such selection.

Action, **Pass** – A webpage which content matches with the keyword object /group selection listed in this field is allowed to be passed through the router.

Action, Block - A webpage which content matches with the keyword object /group selection listed in this field is blocked through the router.

Action

Pass - Allow accessing into the corresponding webpage with the categories listed on the box below.

Block - Restrict accessing into the corresponding webpage with the categories listed on the box below.

If the web pages do not match with the specified feature set here, it will be processed with reverse action.

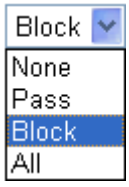
Log

None – There is no log file will be recorded for this profile.

Pass – Only the log about Pass will be recorded in Syslog.

Block – Only the log about Block will be recorded in Syslog.

All – All the actions (Pass and Block) will be recorded in Syslog.



For this section, please refer to **Web Content Filter** user's guide for more information.

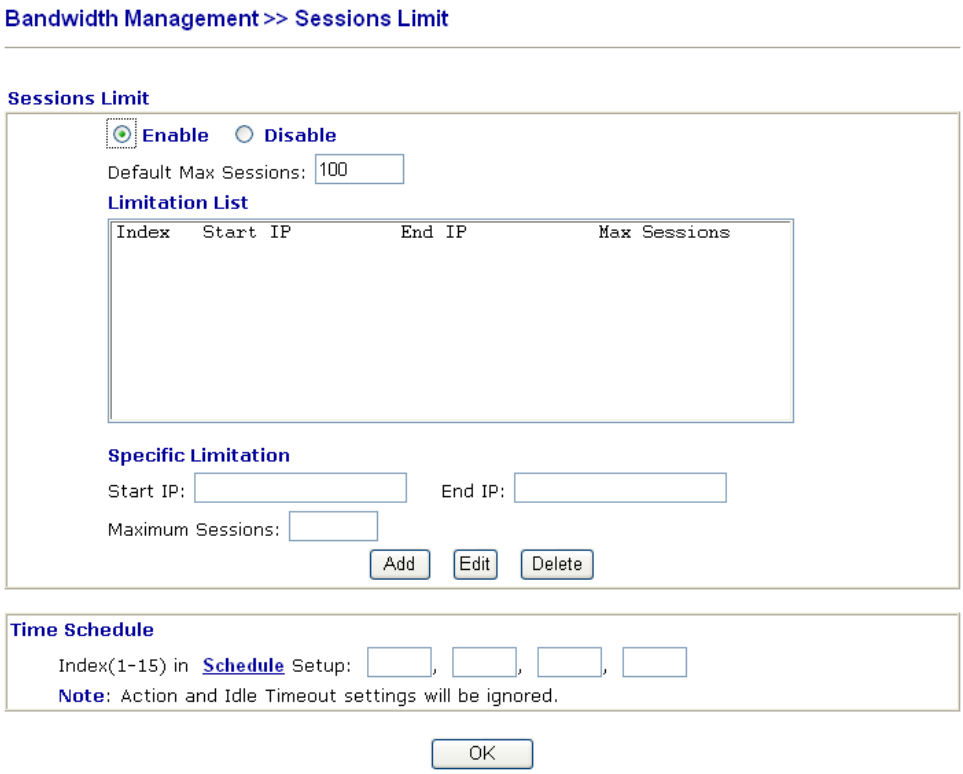
3.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

3.7.1 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.



To activate the function of limit session, simply click **Enable** and set the default session limit.

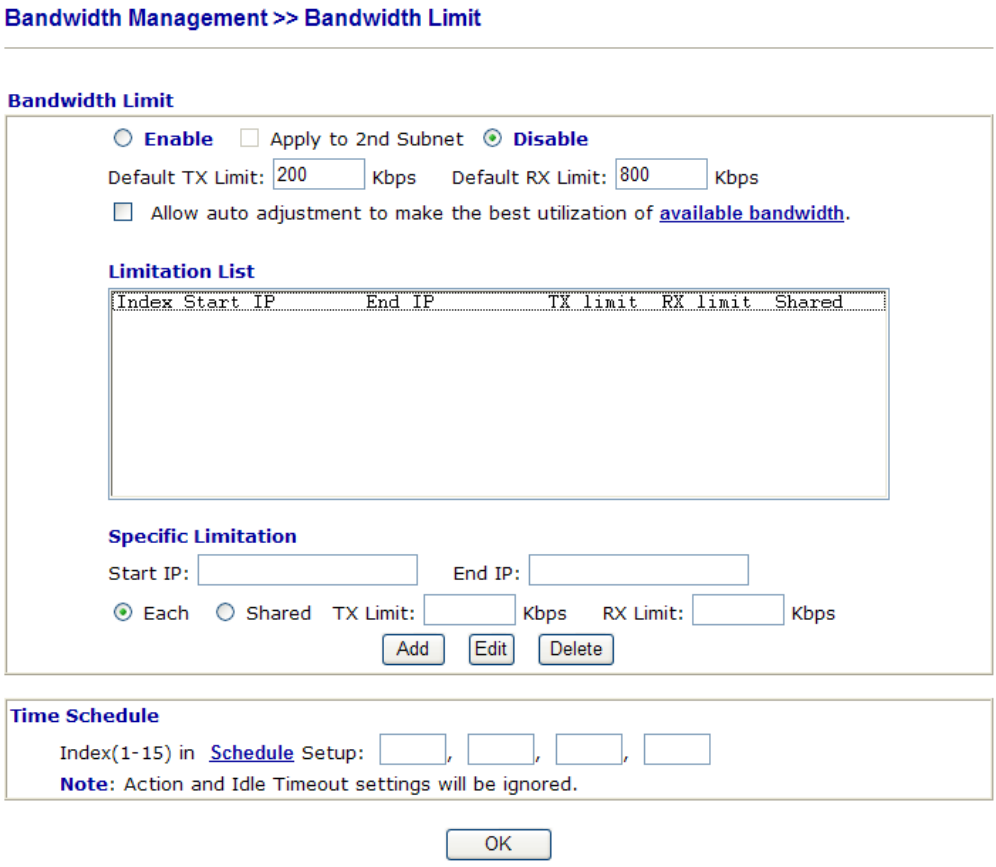
Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.

Default session limit	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.
Maximum Sessions	Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
Add	Adds the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Remove	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

3.7.2 Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.



To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Enable	Click this button to activate the function of limit bandwidth. **Apply to 2nd Subnet** – Check this box to apply the bandwidth limit to the second subnet specified in **LAN>>General Setup**.
Disable	Click this button to close the function of limit bandwidth.
Default TX limit	Define the default speed of the upstream for each computer in LAN.
Default RX limit	Define the default speed of the downstream for each computer in LAN.
Allow auto adjustment to make the best utilization of available bandwidth	Router will detect if there is enough bandwidth remained for using according to the bandwidth limit set by the user. If yes, the router will adjust the available bandwidth for users to enhance the total utilization.
Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Bandwidth limit can be applied on certain IP range. That's, only the PCs within the range will be influenced by the bandwidth limitation set here. Please define the start IP address for the specific limitation.
End IP	Define the end IP address for the specific limitation.
Each /Shared	Click the radio button to determine the specific limitation will be applied to.
TX limit	Define the limitation for the speed of the upstream to be applied as specific limitation. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit	Define the limitation for the speed of the downstream to be applied as specific limitation.. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Add	Add the specific speed limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Delete	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

3.7.3 Quality of Service

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

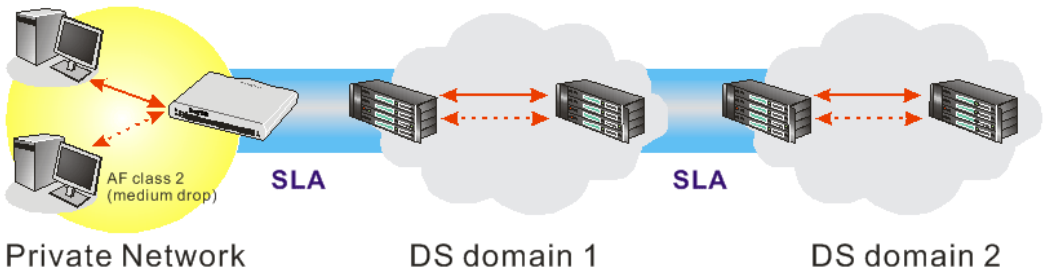
There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

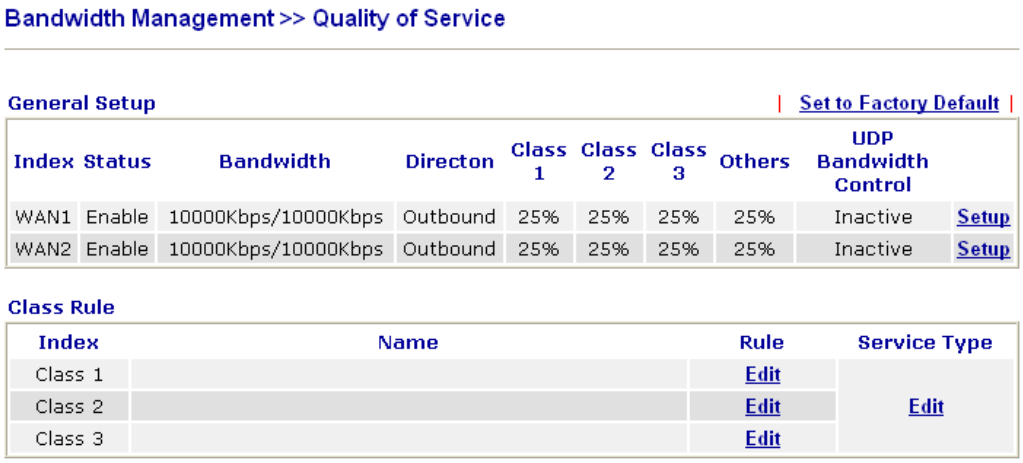
One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

In the **Bandwidth Management** menu, click **Quality of Service** to open the web page.

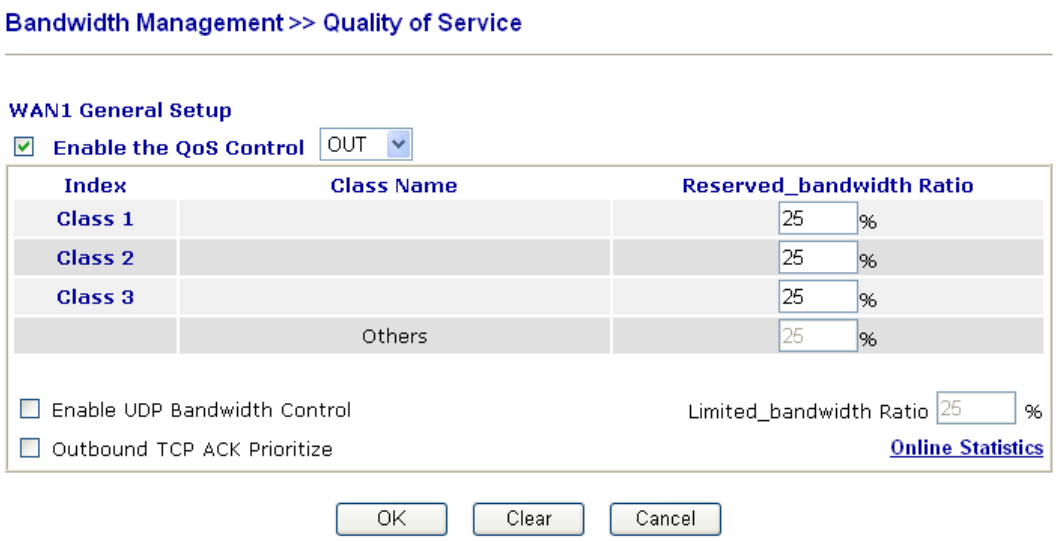

Bandwidth Management >> Quality of Service
General Setup
Set to Factory Default
Index Status Bandwidth Directon Class 1 Class 2 Class 3 Others UDP Bandwidth Control
WAN1 Enable 10000Kbps/10000Kbps Outbound 25% 25% 25% 25% Inactive Setup
WAN2 Enable 10000Kbps/10000Kbps Outbound 25% 25% 25% 25% Inactive Setup
Class Rule
Index Name Rule Service Type
Class 1 Edit
Class 2 Edit Edit
Class 3 Edit

This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN (1/2) interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

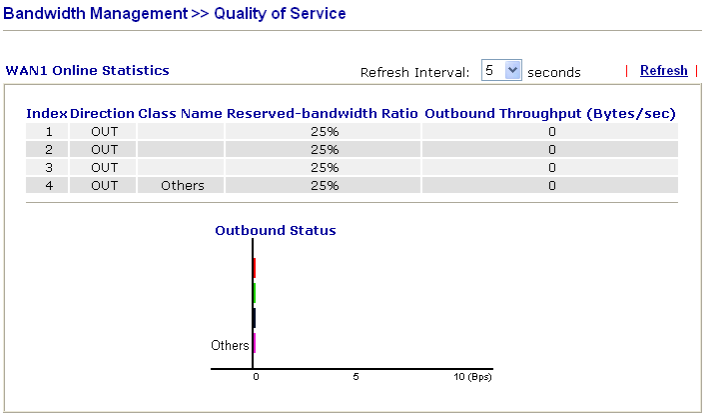
General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.



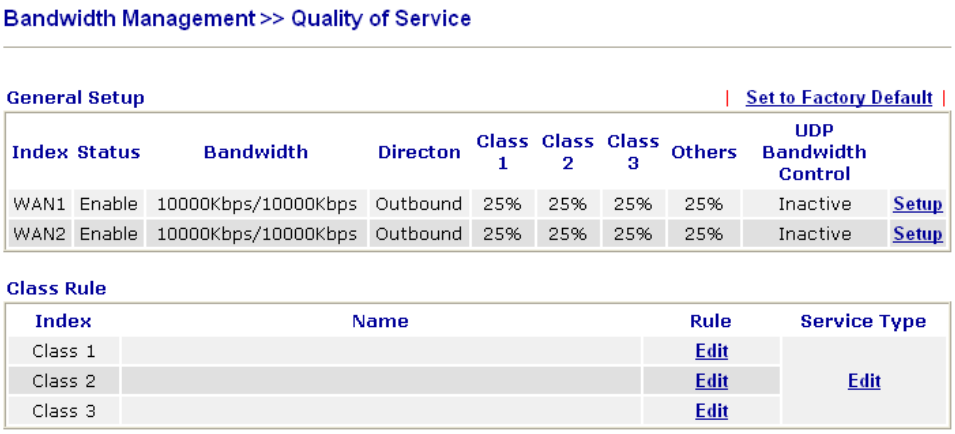
Enable the QoS Control The factory default for this setting is checked.
Please also define which traffic the QoS Control settings will apply to.
IN- apply to incoming traffic only.

	OUT-apply to outgoing traffic only. **BOTH**- apply to both incoming and outgoing traffic. Check this box and click **OK**, then click **Setup** link again. You will see the **Online Statistics** link appearing on this page.
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 10000kbps for this box. The default value is 10000kbps.
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of **reserved bandwidth to upstream speed** and **reserved bandwidth to downstream speed**.
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.
Online Statistics	Display an online statistics for quality of service for your reference. This link will be seen only if you click **OK** in WAN1/WAN2 General Setup web page and click Setup again (for WAN1/WAN2) on the **Bandwidth Management>>Quality of Service**.

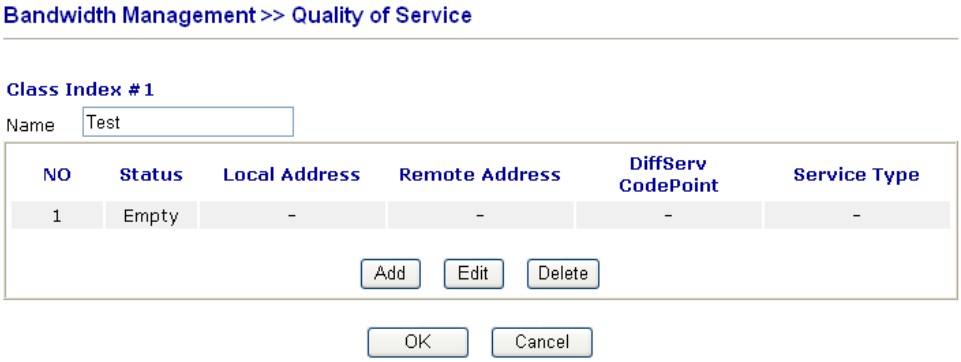


Edit the Class Rule for QoS

The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.


Bandwidth Management >> Quality of Service
General Setup
Set to Factory Default
Index Status Bandwidth Directon Class 1 Class 2 Class 3 Others UDP Bandwidth Control
WAN1 Enable 10000Kbps/10000Kbps Outbound 25% 25% 25% 25% Inactive Setup
WAN2 Enable 10000Kbps/10000Kbps Outbound 25% 25% 25% 25% Inactive Setup
Class Rule
Index Name Rule Service Type
Class 1 Edit
Class 2 Edit Edit
Class 3 Edit

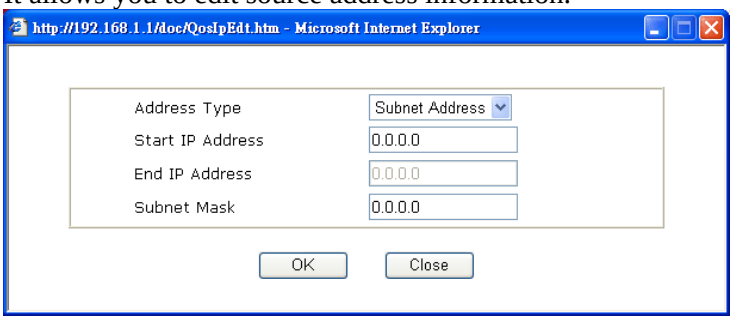
After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, "Test" is used as the name of Class Index #1.


Bandwidth Management >> Quality of Service
Class Index #1
Name Test
NO Status Local Address Remote Address DiffServ CodePoint Service Type
1 Empty - - - -
Add Edit Delete
OK Cancel

For adding a new rule, click **Add** to open the following page.

ACT	Check this box to invoke these settings.
Local Address	Click the **Edit** button to set the local IP address (on LAN) for the rule.
Remote Address	Click the **Edit** button to set the remote IP address (on LAN/WAN) for the rule.

Edit It allows you to edit source address information.

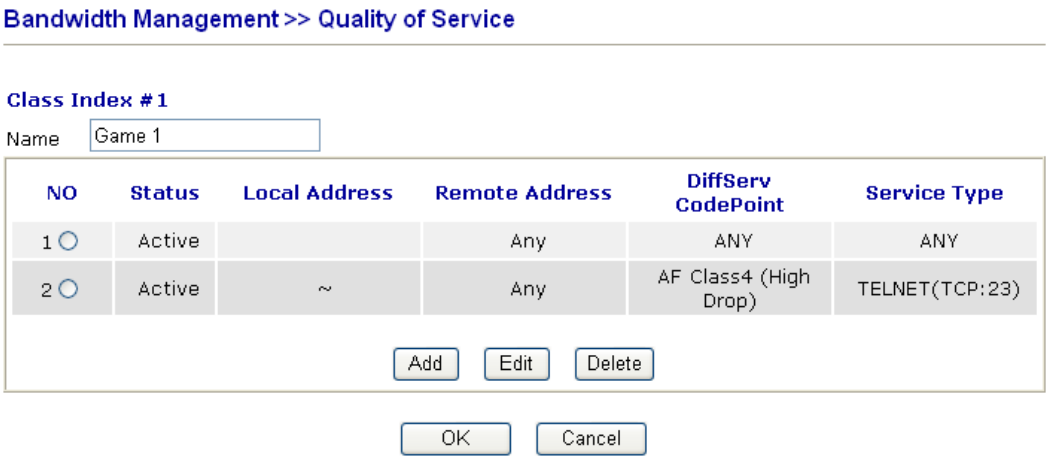


Address Type – Determine the address type for the source address.
For **Single Address**, you have to fill in Start IP address.
For **Range Address**, you have to fill in Start IP address and End IP address.
For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.

DiffServ CodePoint All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.

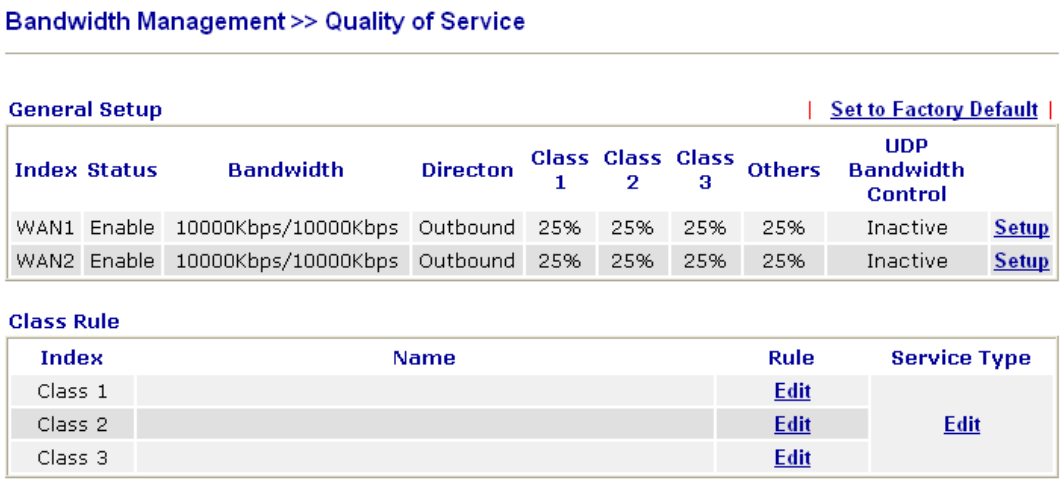
Service Type It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

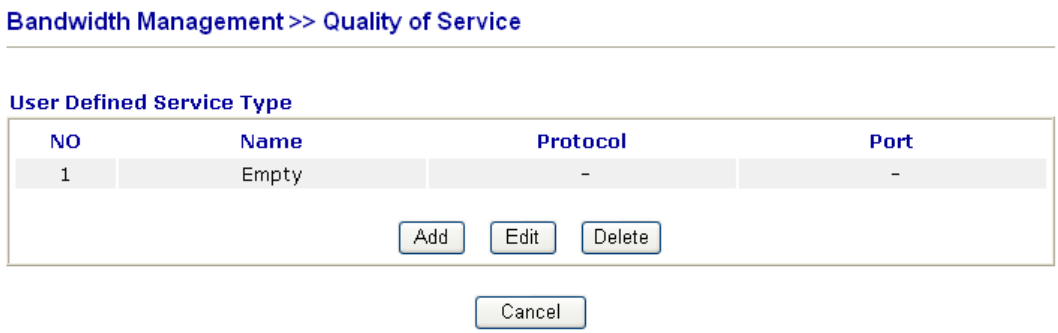


Edit the Service Type for Class Rule

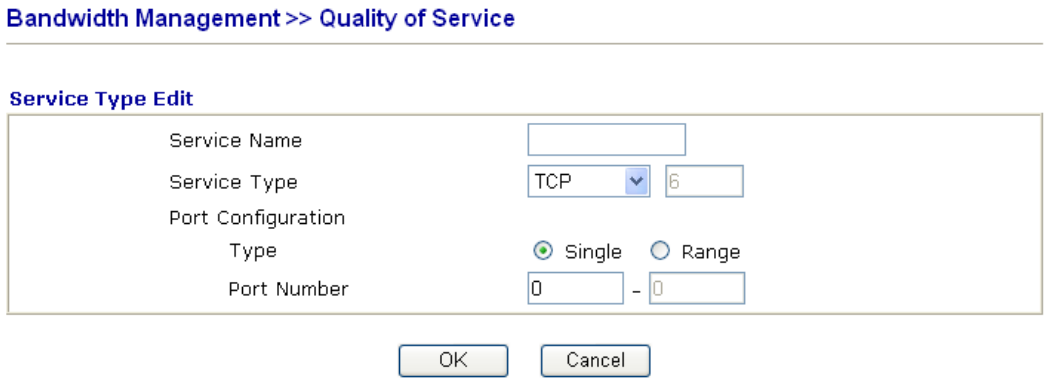
To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.


Bandwidth Management >> Quality of Service
General Setup
Set to Factory Default
Index Status Bandwidth Directon Class 1 Class 2 Class 3 Others UDP Bandwidth Control
WAN1 Enable 10000Kbps/10000Kbps Outbound 25% 25% 25% 25% Inactive Setup
WAN2 Enable 10000Kbps/10000Kbps Outbound 25% 25% 25% 25% Inactive Setup
Class Rule
Index Name Rule Service Type
Class 1 Edit
Class 2 Edit Edit
Class 3 Edit

After you click the **Edit** link, you will see the following page.



For adding a new service type, click **Add** to open the following page.



Service Name Type in a new service for your request.

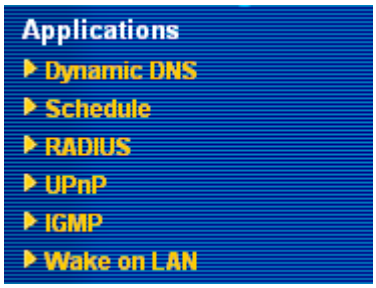
Service Type Choose the type (TCP, UDP or TCP/UDP) for the new service.

Port Configuration Click **Single** or **Range** as the **Type**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.
Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.

By the way, you can set up to 40 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

3.8 Applications

Below shows the menu items for Applications.



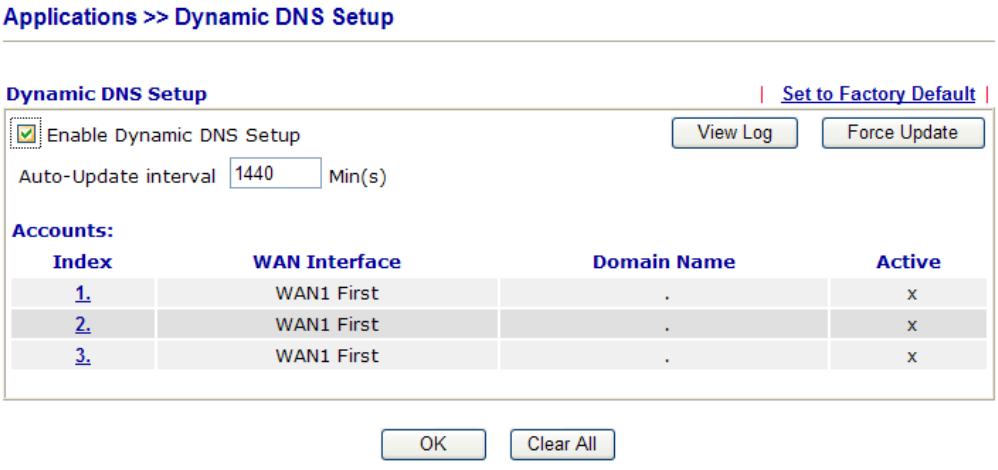
3.8.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com.** You should visit their websites to register your own domain name for the router.

Enable the Function and Add a Dynamic DNS Account

1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
2. In the DDNS setup menu, check **Enable Dynamic DNS Setup**.



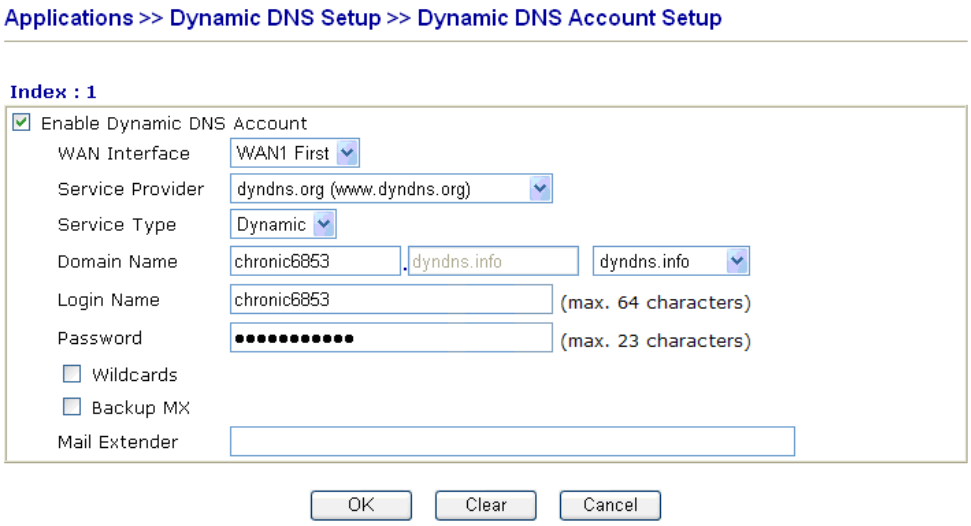
Set to Factory Default Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup Check this box to enable DDNS function.

Auto-Update interval Set the time for the router to perform auto update for DDNS service.

Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
WAN Interface	Display current WAN interface used for accessing Internet.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

3. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.



Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	Select the WAN interface order to apply settings here.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

4. Click **OK** button to activate the settings. You will see your setting has been saved.

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

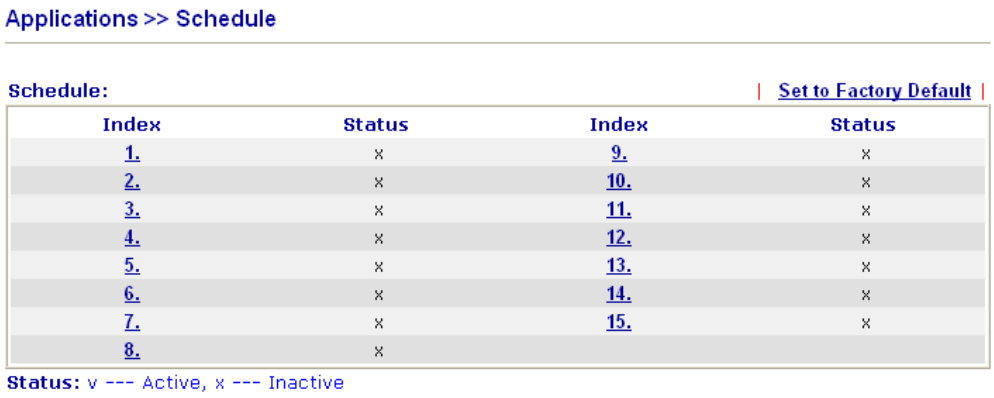
Delete a Dynamic DNS Account

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

3.8.2 Schedule

The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

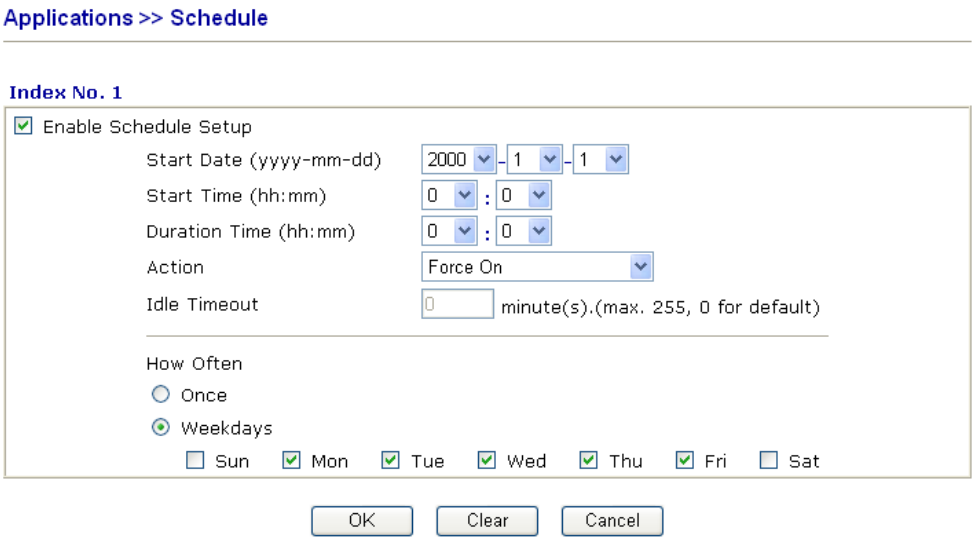
You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.



Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page of schedule.
Status	Display if this schedule setting is active or inactive.

You can set up to 15 schedules. Then you can apply them to your **Internet Access** or **VPN and Remote Access >> LAN-to-LAN** settings.

To add a schedule, please click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown below.



Enable Schedule Setup	Check to enable the schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
Action	Specify which action Call Schedule should apply during the period of the schedule. **Force On** -Force the connection to be always on. **Force Down** -Force the connection to be always down. **Enable Dial-On-Demand** -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field. **Disable Dial-On-Demand** -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.
Idle Timeout	Specify the duration (or period) for the schedule. **How often** -Specify how often the schedule will be applied **Once** -The schedule will be applied just once **Weekdays** -Specify which days in one week should perform the schedule.

Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).

Office Hour:

(Force On)

Mon - Sun **9:00 am** **to** **6:00 pm**

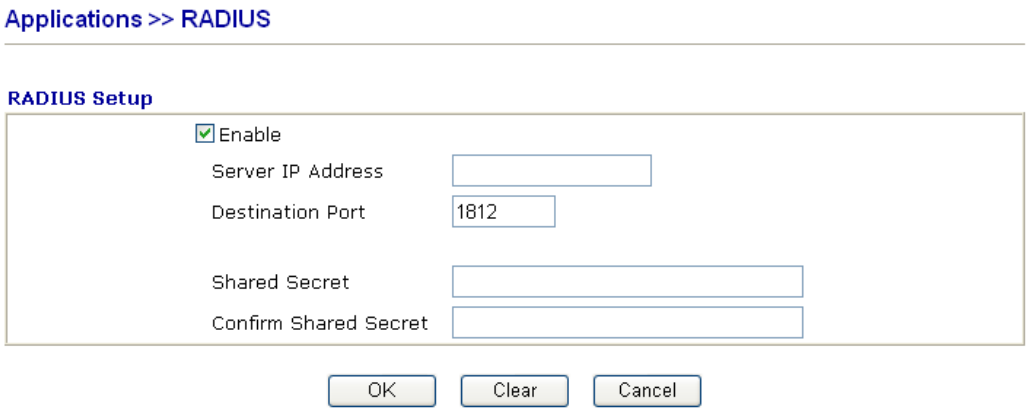
1. Make sure the PPPoE connection and **Time Setup** is working properly.

2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

3.8.3 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

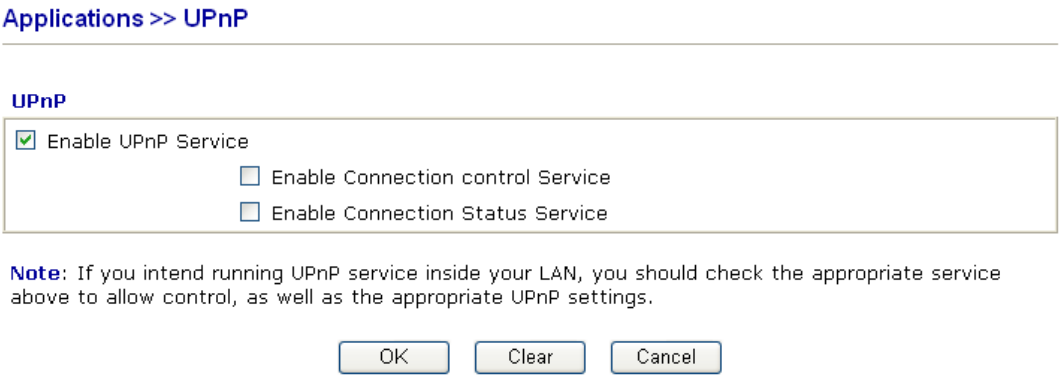
The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.



Enable	Check to enable RADIUS client feature
Server IP Address	Enter the IP address of RADIUS server
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

3.8.4 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is “NAT Traversal”. This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

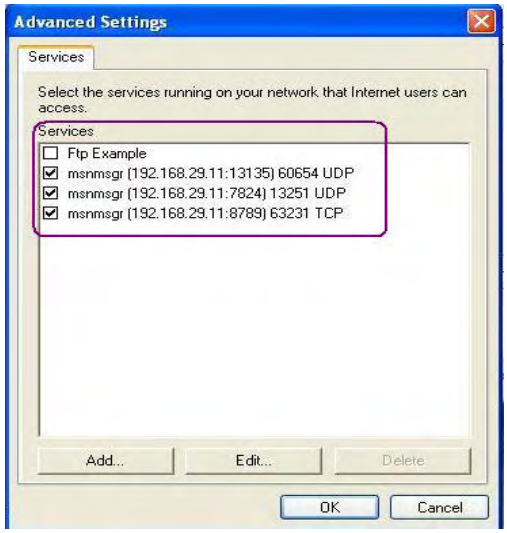

Applications >> UPnP
UPnP
Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service
Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.
OK
Clear
Cancel

Enable UPNP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.

The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.

IP Broadband Connection on Router Properties
General
Connect to the Internet using:
IP Broadband Connection on Router
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel



The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

Security Considerations

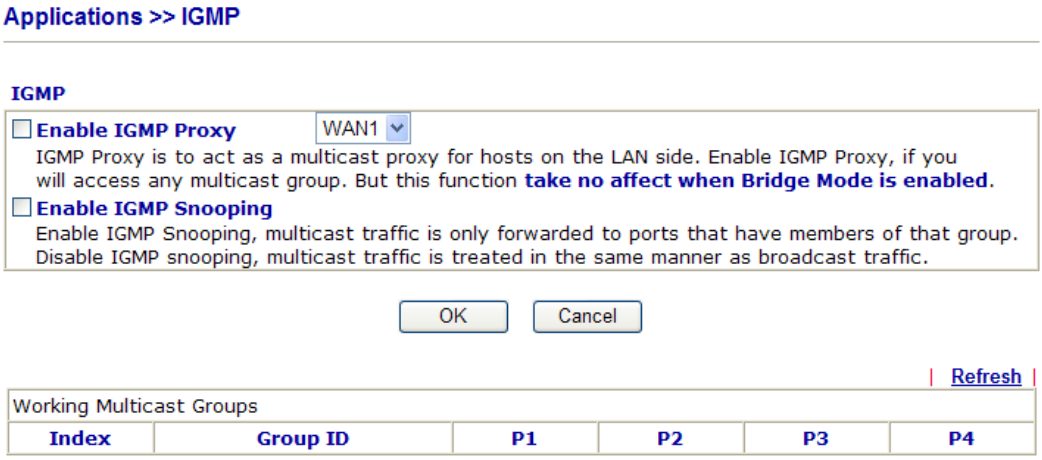
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

3.8.5 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. For invoking IGMP Snooping function, you have to check the Enable IGMP Proxy box first for activating the IGMP proxy function.


Applications >> IGMP
IGMP
Enable IGMP Proxy
WAN1
IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function take no affect when Bridge Mode is enabled.
Enable IGMP Snooping
Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.
OK
Cancel
Refresh
Working Multicast Groups
Index
Group ID
P1
P2
P3
P4

Enable IGMP Proxy Check this box to enable this function. The application of multicast will be executed through WAN1/2 port or PVC. Use the drop down list to choose the interface.

Enable IGMP Snooping Check this box to enable this function. The application of multicast will be executed for the clients in LAN.

Group ID This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.

P1 to P4 It indicates the LAN port used for the multicast group.

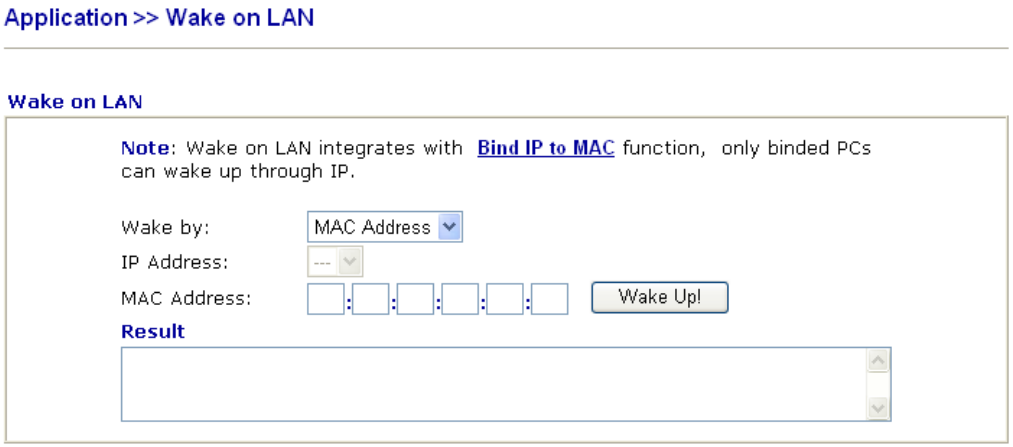
Refresh Click this link to renew the working multicast group status.

If you check Enable IGMP Proxy, you will get the following page. All the multicast groups will be listed and all the LAN ports (P1 to P4) are available for use.

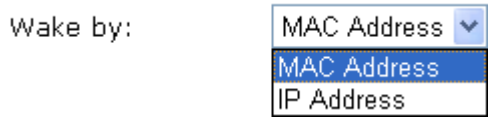
3.8.6 Wake on LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake on LAN** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as “Enable” on the BIOS setting.



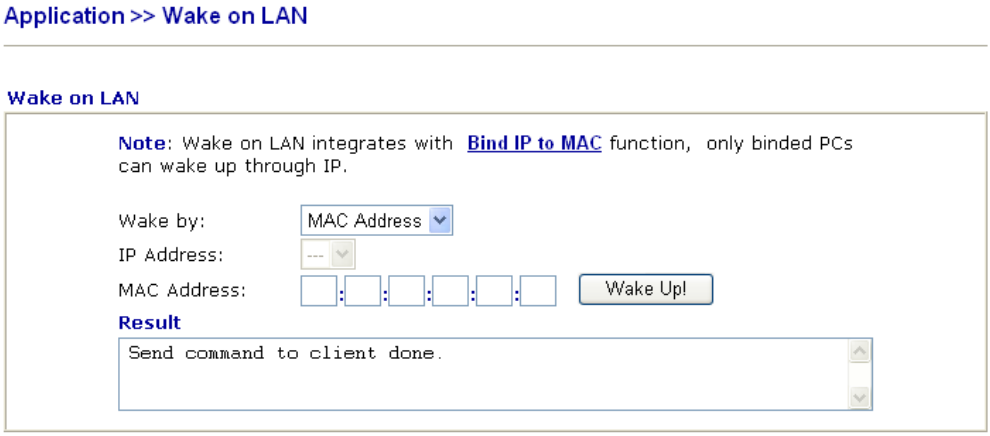
Wake by Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.



IP Address The IP addresses that have been configured in **Firewall>>Bind IP to MAC** will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.

MAC Address Type any one of the MAC address of the binded PCs.

Wake Up Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.

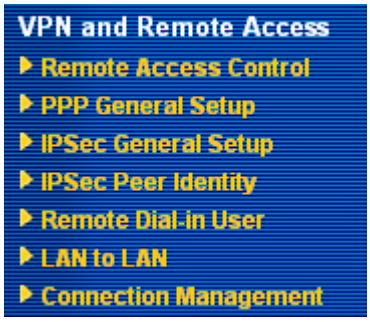

Application >> Wake on LAN
Wake on LAN
Note: Wake on LAN integrates with Bind IP to MAC function, only binded PCs can wake up through IP.
Wake by:
MAC Address
IP Address:

MAC Address:
Wake Up!
Result
Send command to client done.

3.9 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

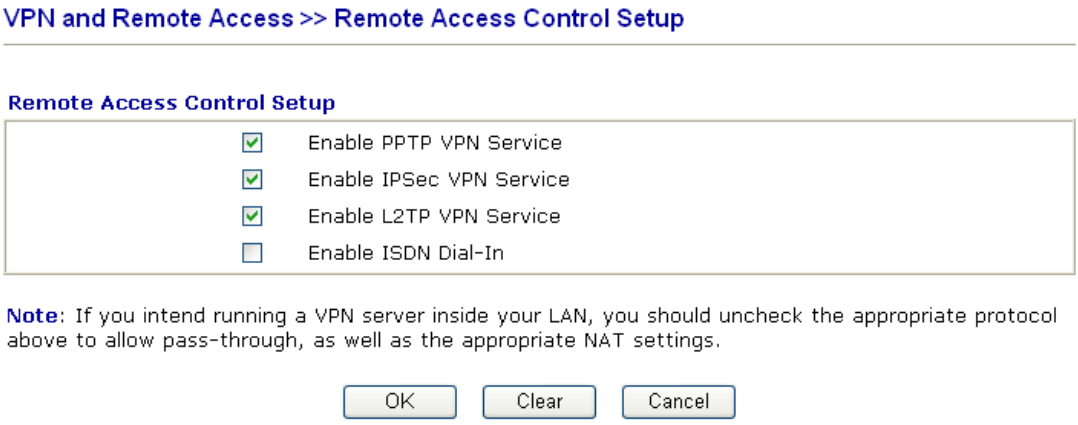
Below shows the menu items for VPN and Remote Access.



Note: This feature can be applied for ISDN remote dial-in or ISDN LAN-to-LAN connection in *n* series models.

3.9.1 Remote Access Control

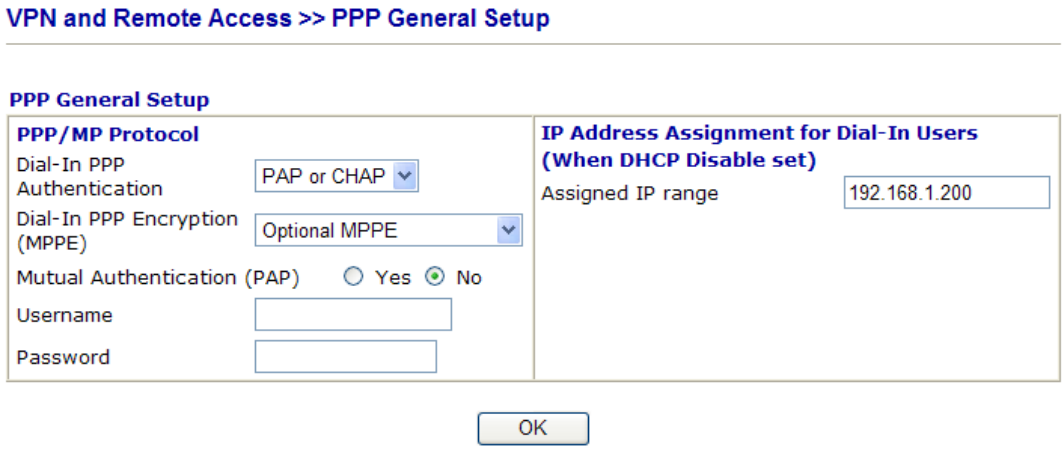
Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.


VPN and Remote Access >> Remote Access Control Setup
Remote Access Control Setup
Enable PPTP VPN Service
Enable IPSec VPN Service
Enable L2TP VPN Service
Enable ISDN Dial-In
Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.
OK
Clear
Cancel

The Vigor router will not accept the ISDN dial-in connection if the box of **Enable ISDN Dial-in** is not checked.

3.9.2 PPP General Setup

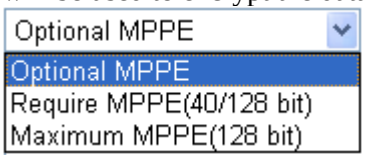
This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.



Dial-In PPP Authentication PAP Only
Select this option to force the router to authenticate dial-in users with the PAP protocol.

PAP or CHAP
Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.

Dial-In PPP Encryption (MPPE Optional MPPE
This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.



Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.
Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.

Mutual Authentication (PAP)
The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the **User Name** and **Password** of the mutual authentication peer.

Assigned IP Address Enter a specific IP address for the dial-in PPP connection. You should choose an IP address from the local private network.

3.9.3 IPSec General Setup

In **IPSec General Setup,** there are two major parts of configuration.

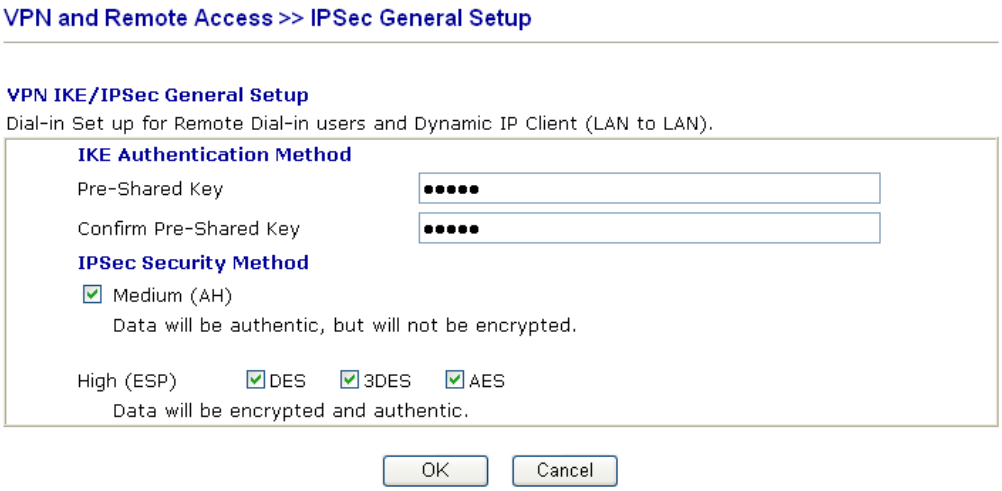
There are two phases of IPSec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPSec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.



IKE Authentication Method This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.
Pre-Shared Key -Currently only support Pre-Shared Key authentication.
Pre-Shared Key- Specify a key for IKE authentication

Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.

IPSec Security Method

Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.

High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

3.9.4 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **32** entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPSec Peer Identity

X509 Peer ID Accounts: | Set to Factory Default |

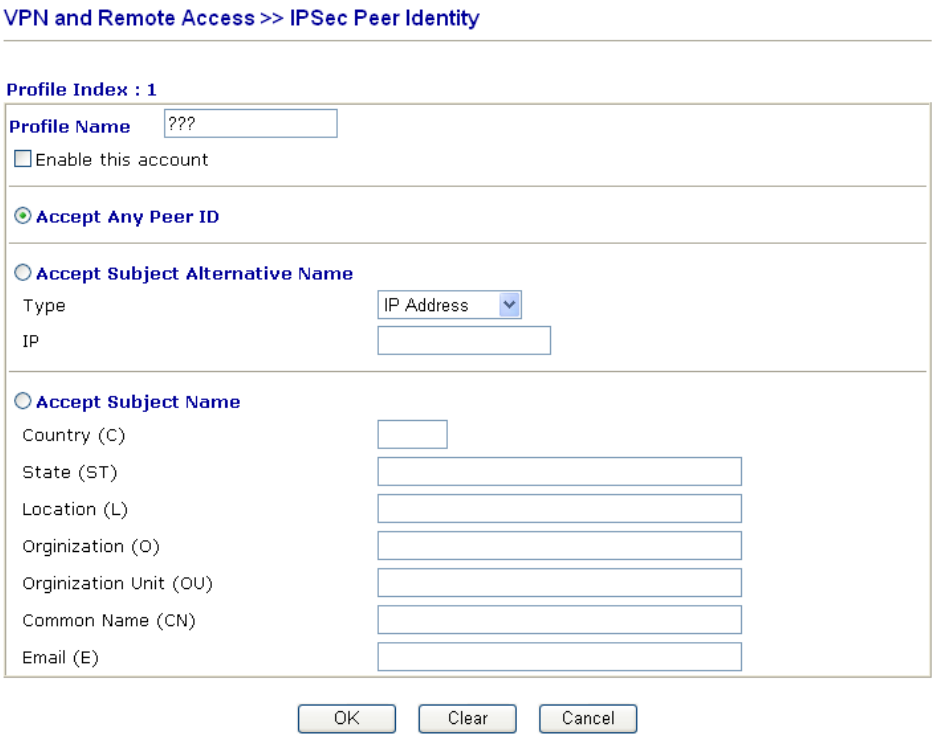
Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Set to Factory Default Click it to clear all indexes.

Index Click the number below Index to access into the setting page of IPSec Peer Identity.

Name Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

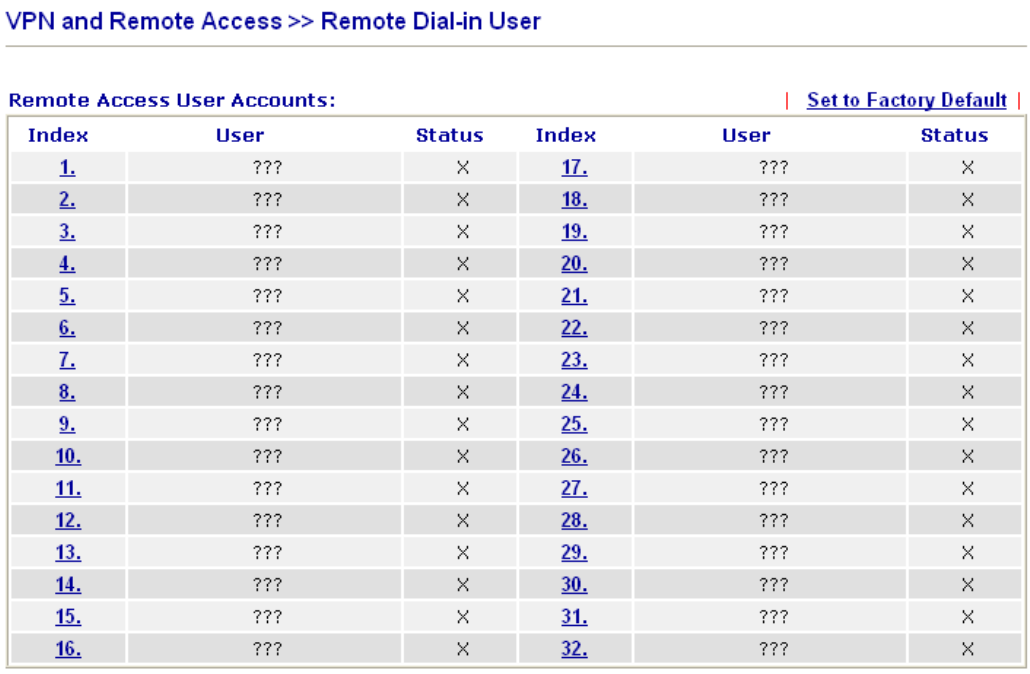


Profile Name	Type in a name in this file.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address, Domain,** or **E-mail Address**. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN),** and **Email (E)**.

3.9.5 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via ISDN or build the VPN connection. You may set parameters including specified connection peer ID, connection type (ISDN Dial-In connection, VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

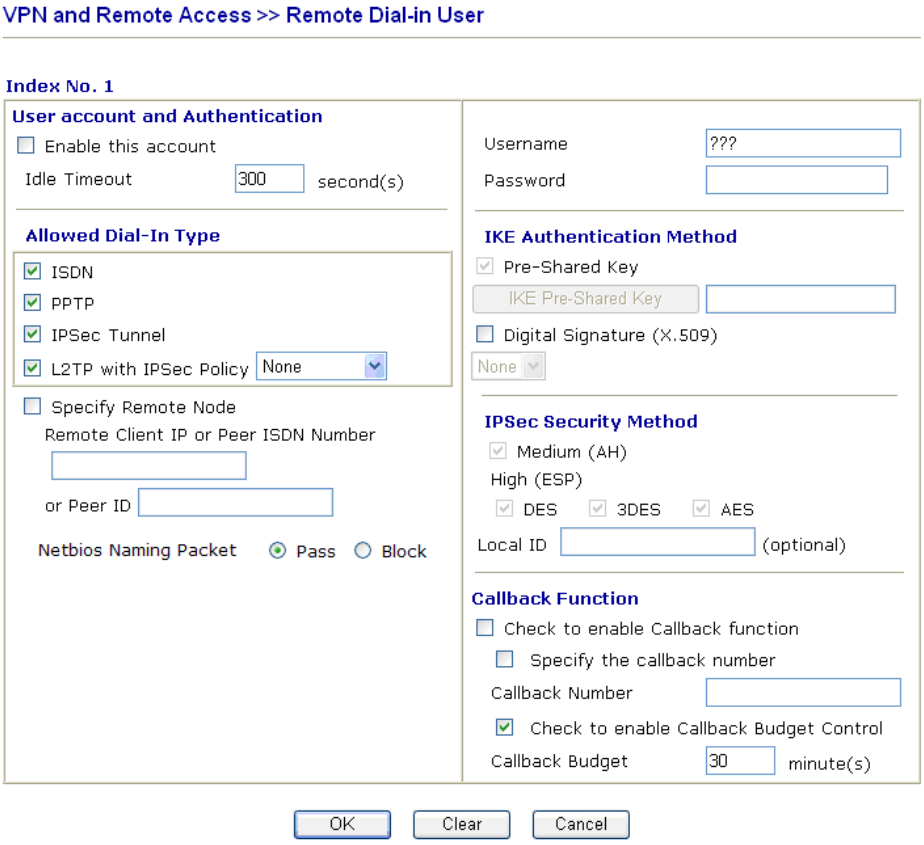
The router provides **32** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.



Index	User	Status	Index	User	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.



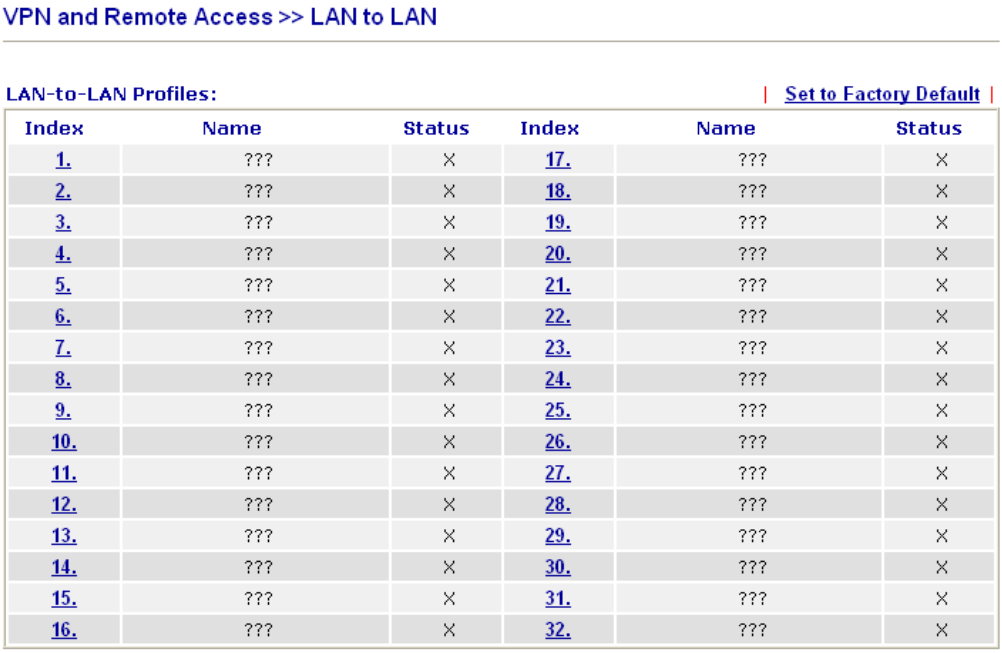
Enable this account	Check the box to enable this function. **Idle Timeout-** If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
ISDN	Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below. This feature is for ***n*** model only.
PPTP	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below
IPSec Tunnel	Allow the remote dial-in user to make an IPSec VPN connection through Internet.
L2TP	Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: **None -** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. **Nice to Have -** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. **Must -**Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify Remote Node	**Check the checkbox-**You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE

	aggressive mode). **Uncheck the checkbox**-This means the connection type you select above will apply the authentication methods and security methods in the **general settings**.
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. **Pre-Shared Key** - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. **Digital Signature (X.509) –** Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity.**
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. **Medium -Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. **High-Encapsulating Security Payload (ESP)** means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. **Local ID** - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.
Callback Function	The callback function provides a callback service only for the ISDN dial-in user (for *s* model only). The remote user will be charged the connection fee by the telecom. **Check to enable Callback function**-Enables the callback function. **Specify the callback number**-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. **Check to enable callback budget control**-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically. **Callback Budget (Unit: minutes)**- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.9.6 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router supports 2 VPN tunnels and provides up to **32** profiles simultaneously. The following figure shows the summary table.

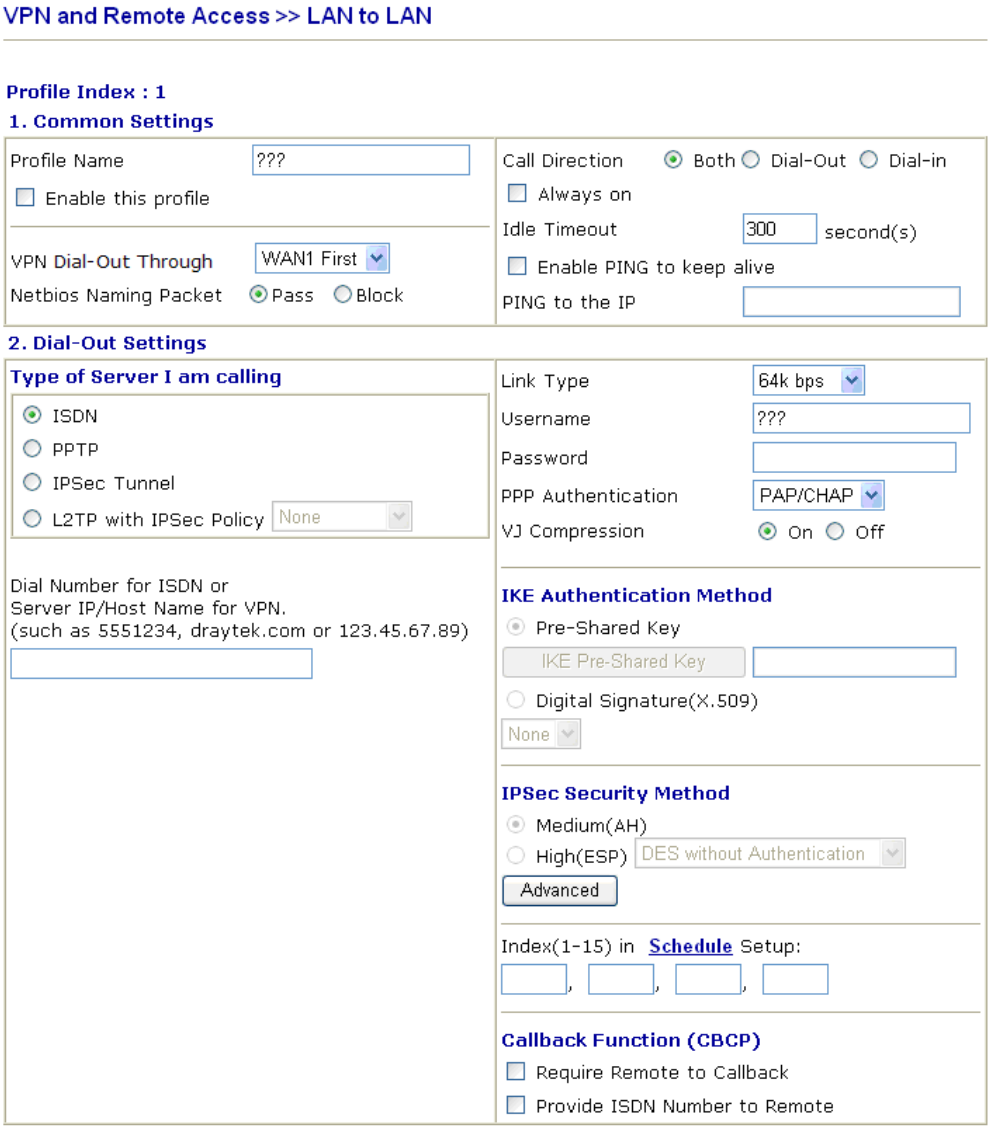


Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

For the web page is too long, we divide the page into several sections for explanation.

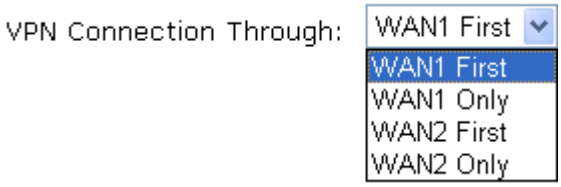


Profile Name Specify a name for the profile of the LAN-to-LAN connection.

Enable this profile Check here to activate this profile.

Netbios Naming Packet **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

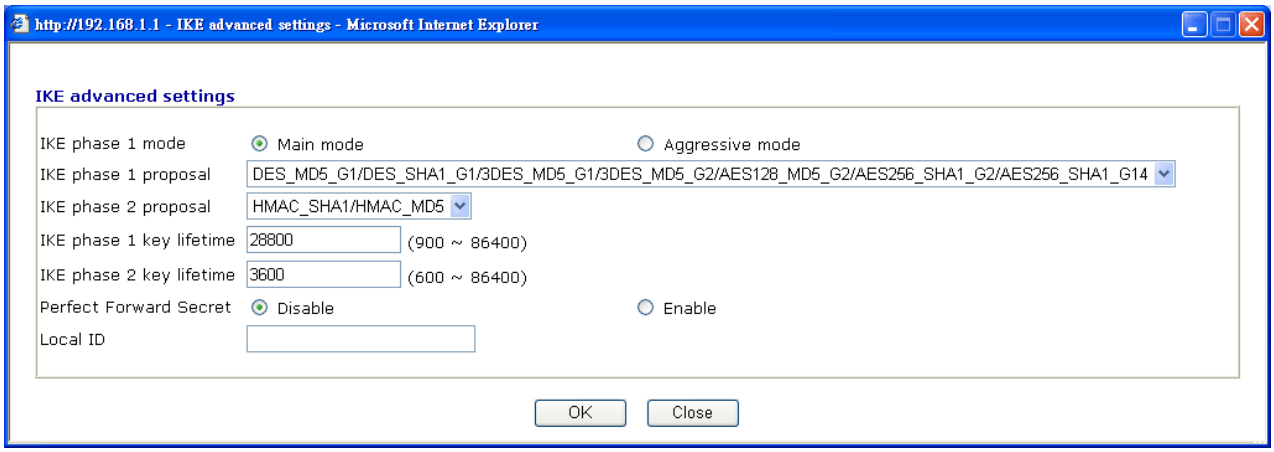
VPN Dial-Out Through Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.



WAN1 First - While connecting, the router will use WAN1 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.

	WAN1 Only - While connecting, the router will use WAN1 as the only channel for VPN connection. **WAN2 First** - While connecting, the router will use WAN2 as the first channel for VPN connection. If WAN2 fails, the router will use another WAN interface instead. **WAN2 Only** - While connecting, the router will use WAN2 as the only channel for VPN connection.
Netbios Naming Packet	**Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. **Both**:-initiator/responder **Dial-Out**- initiator only **Dial-In-** responder only.
Always On or Idle Timeout	**Always On**-Check to enable router always keep VPN connection. **Idle Timeout:** The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
	Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
ISDN	Build ISDN LAN-to-LAN connection to remote network. You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below. This feature is useful for *s* model only.
PPTP	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.

IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.
L2TP with …	Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: **None:** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. **Nice to Have:** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. **Must:** Specify the IPSec policy to be definitely applied on the L2TP connection.
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
PPP Authentication	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy. **Pre-Shared Key** - Input 1-63 characters as pre-shared key. **Digital Signature (X.509)** - Select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.
Medium	**Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is active. **High (ESP-Encapsulating Security Payload)-** means payload (data) will be encrypted and authenticated. Select from below: **DES without Authentication** -Use DES encryption algorithm and not apply any authentication scheme. **DES with Authentication-**Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. **3DES without Authentication**-Use triple DES encryption algorithm and not apply any authentication scheme. **3DES with Authentication-**Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. **AES without Authentication**-Use AES encryption algorithm and not apply any authentication scheme. **AES with Authentication-**Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
Advanced	Specify mode, proposal and key life of each IKE phase, Gateway etc. The window of advance setup is shown as below:



IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

IKE phase 1 proposal-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.

IKE phase 2 proposal-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.

IKE phase 1 key lifetime-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.

IKE phase 2 key lifetime-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.

Perfect Forward Secret (PFS)-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

Local ID-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

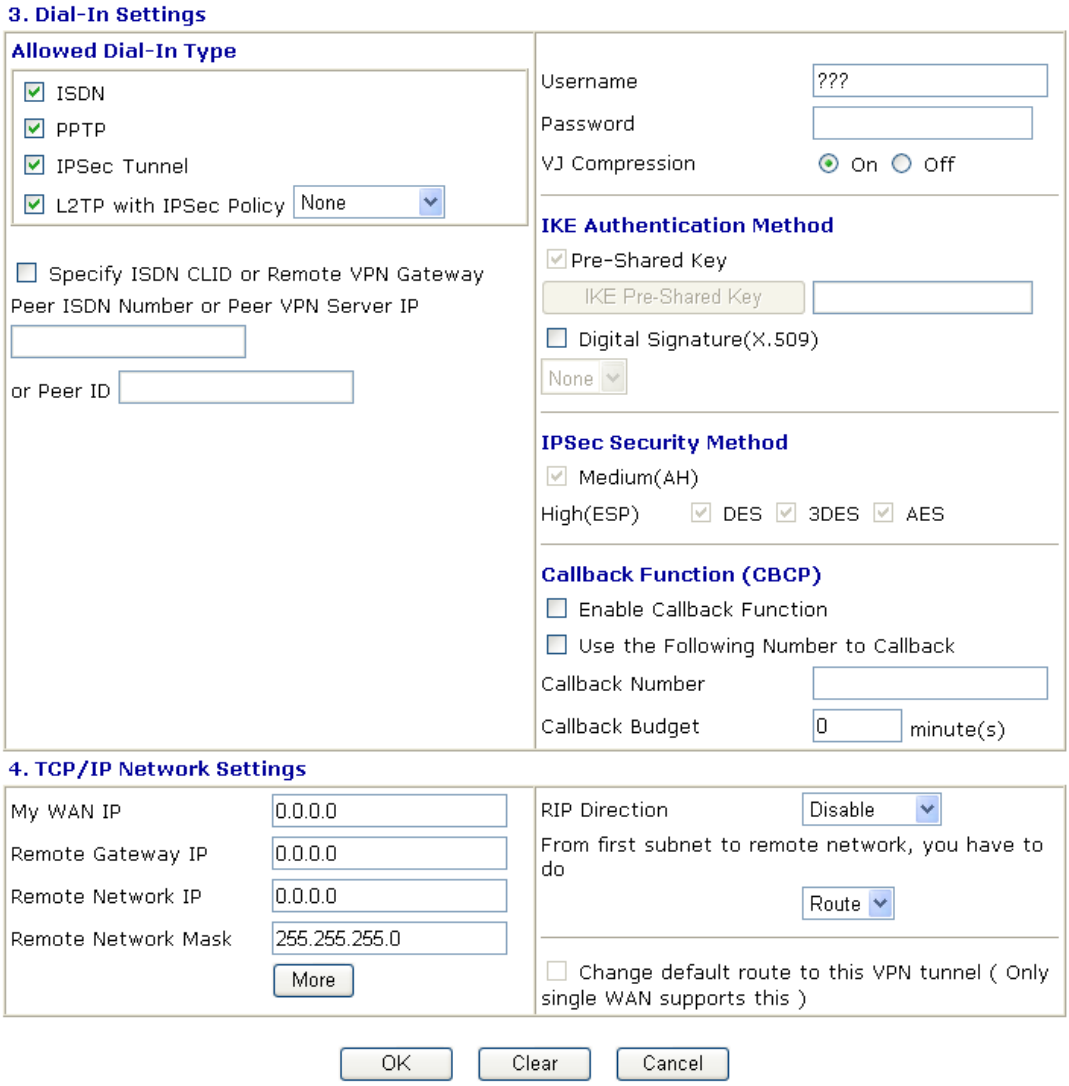
Callback Function (for *s* models only)

The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.

Require Remote to Callback-Enable this to let the router to require the remote peer to callback for the connection afterwards.

Provide ISDN Number to Remote-In the case that the remote peer requires the Vigor router to callback, the local ISDN number will be provided to the remote peer. Check here to allow the Vigor router to send the ISDN number to

the remote router. This feature is useful for *s* model only.



Allowed Dial-In Type Determine the dial-in connection with different types.

ISDN Allow the remote ISDN LAN-to-LAN connection. You should set the User Name and Password of remote dial-in user below. This feature is useful for *s* model only. In addition, you can further set up Callback function below.

PPTP Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.

IPSec Tunnel Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.

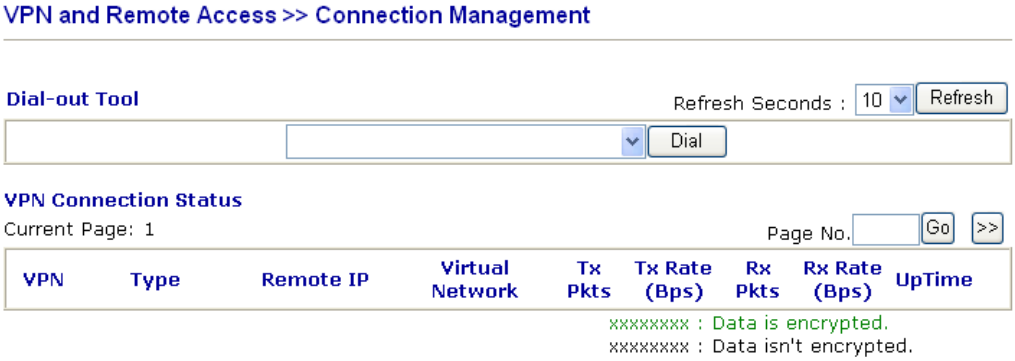
L2TP Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:
None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.
Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection

	becomes one pure L2TP connection. **Must -** Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify CLID or Remote VPN Gateway	You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Peer ISDN number if you select ISDN above (This feature is useful for *n* model only.). Also, you should further specify the corresponding security methods on the right side. If you uncheck the checkbox**,** the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. **Digital Signature (X.509) –**Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. **Medium-** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. **High-** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
Callback Function	The callback function provides a callback service only for the ISDN LAN-to-LAN connection (this feature is useful for *s* model only). The remote user will be charged the connection fee by the telecom. **Check to enable Callback function**-Enables the callback function. **Callback number**-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. **Callback budget**- By default, the callback function has limitation of callback period. Once the callback budget is

	exhausted, the function will be disabled automatically. **Callback Budget (Unit: minutes)-** Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection. The default value 0 means no limitation of callback period.
My WAN IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Gateway IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Network IP/ Remote Network Mask	Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
More	Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
From first subnet to remote network, you have to do	If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.
Change default route to this VPN tunnel	Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled. You have to disable one WAN interface (WAN 1 or WAN 2) on **WAN >> General Setup** for enabling such setting.

3.9.7 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.



Dial	Click this button to execute dial out function.
Refresh Seconds	Choose the time for refresh the dial information among 5, 10, and 30.
Refresh	Click this button to refresh the whole connection status.

3.10 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

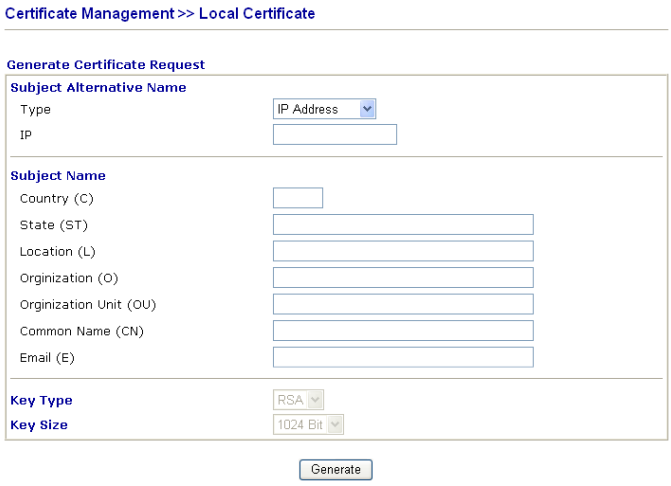
Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

3.10.1 Local Certificate

Generate Click this button to open **Generate Certificate Request** window.



Type in all the information that the window request. Then click **Generate** again.

Import Click this button to import a saved file as the certification information.

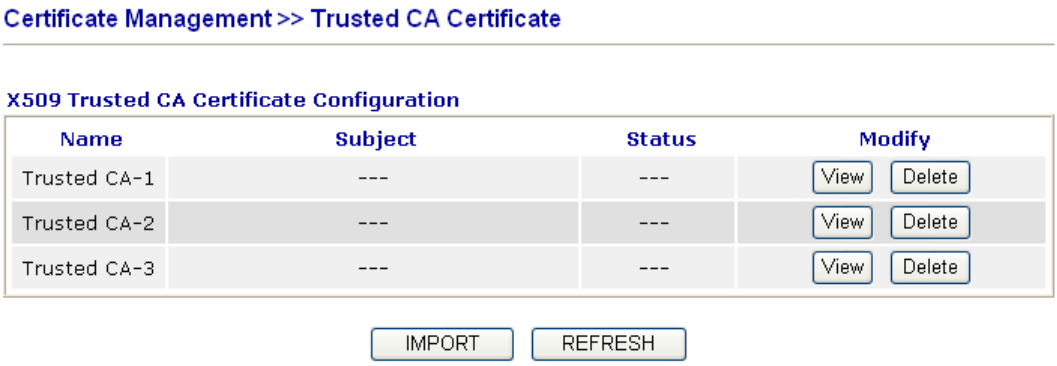
Refresh Click this button to refresh the information listed below.

View Click this button to view the detailed settings for certificate request.

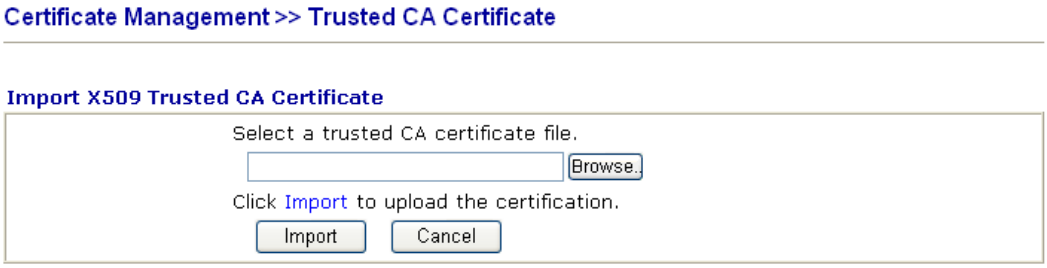
After clicking **Generate**, the generated information will be displayed on the window below:

3.10.2 Trusted CA Certificate

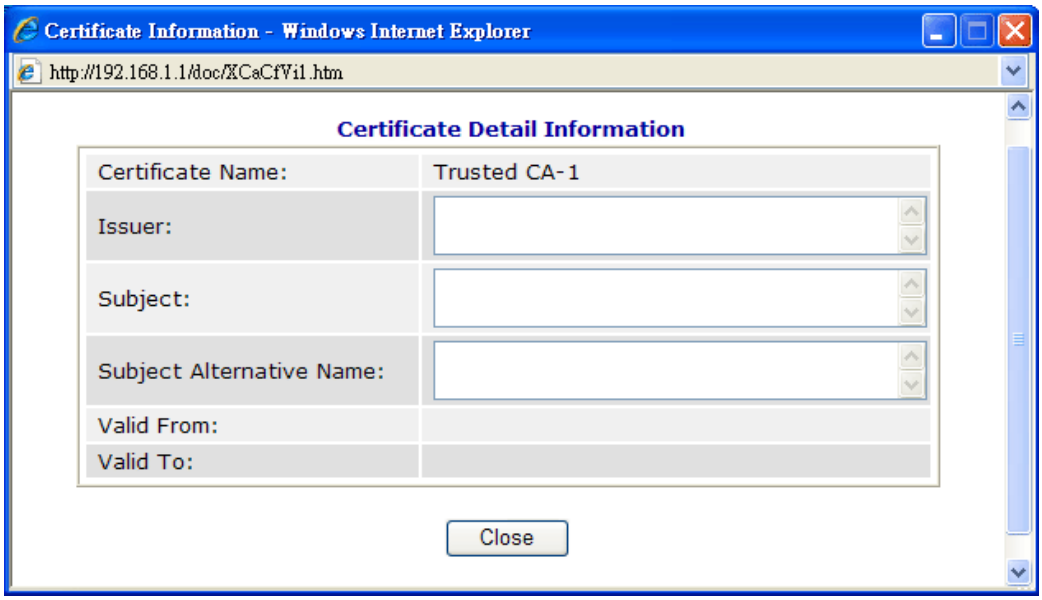
Trusted CA certificate lists three sets of trusted CA certificate.



To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse…** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.



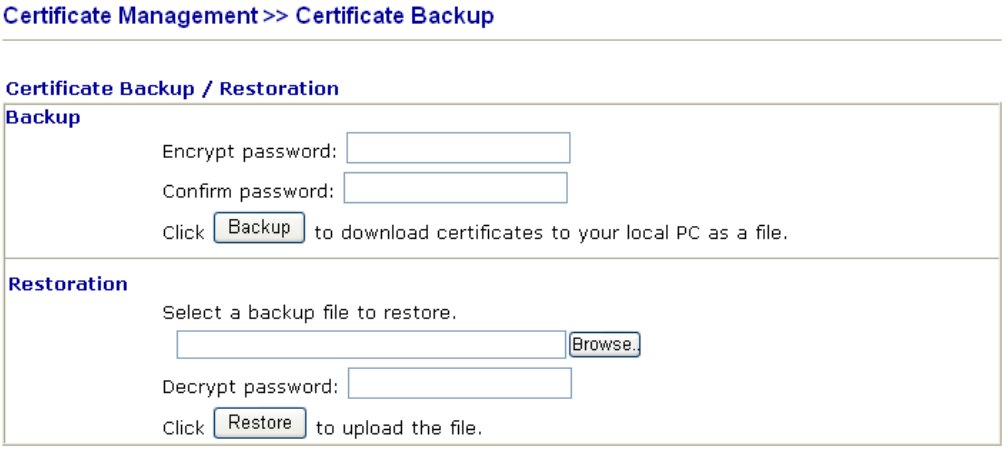
For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



3.10.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.



3.11 VoIP

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, “SIP Address”. The standard format of SIP URI is

sip: user:password @ host: port

Some fields may be optional in different use. In general, "host” refers to a domain. The “userinfo” includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it “SIP URL”. SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN/ISDN network.

After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/μ-law, G.723, G.726 and G.729 A & B. Each codec uses a different bandwidth and hence provides different levels of voice quality. The more bandwidth a codec uses the better the voice quality, however the codec used must be appropriate for your Internet bandwidth.

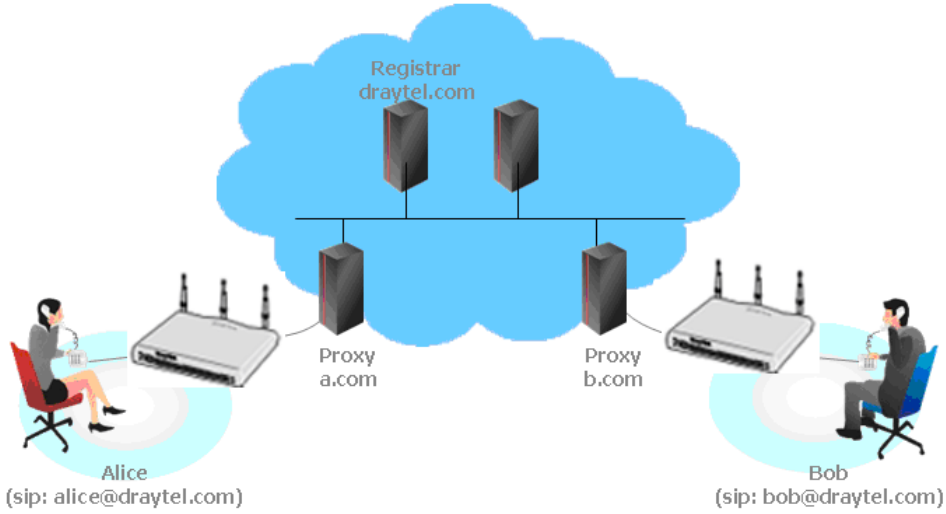
Usually there will be two types of calling scenario, as illustrated below:

- **Calling via SIP Servers**

  First, the Vigor V models of yours will have to register to a SIP Registrar by sending

registration messages to validate. Then, both parties' SIP proxies will forward the sequence of messages to caller to establish the session.

If you both register to the same SIP Registrar, then it will be illustrated as below:

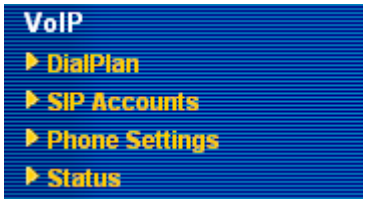


The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer to the **section 4.5.1.**

- **Peer-to-Peer**

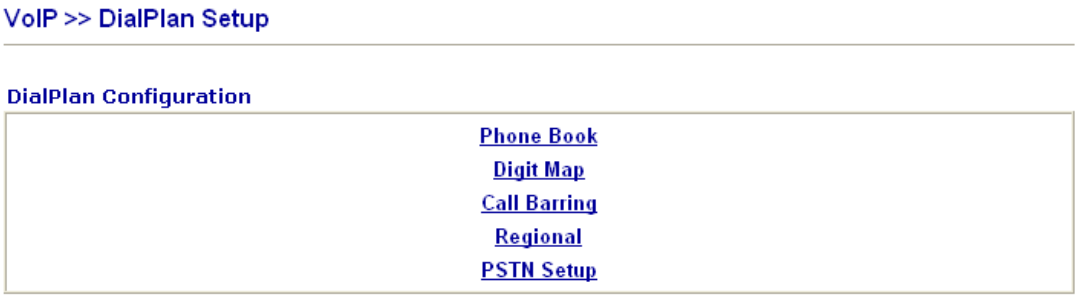
Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **section 4.5.2.**

Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.



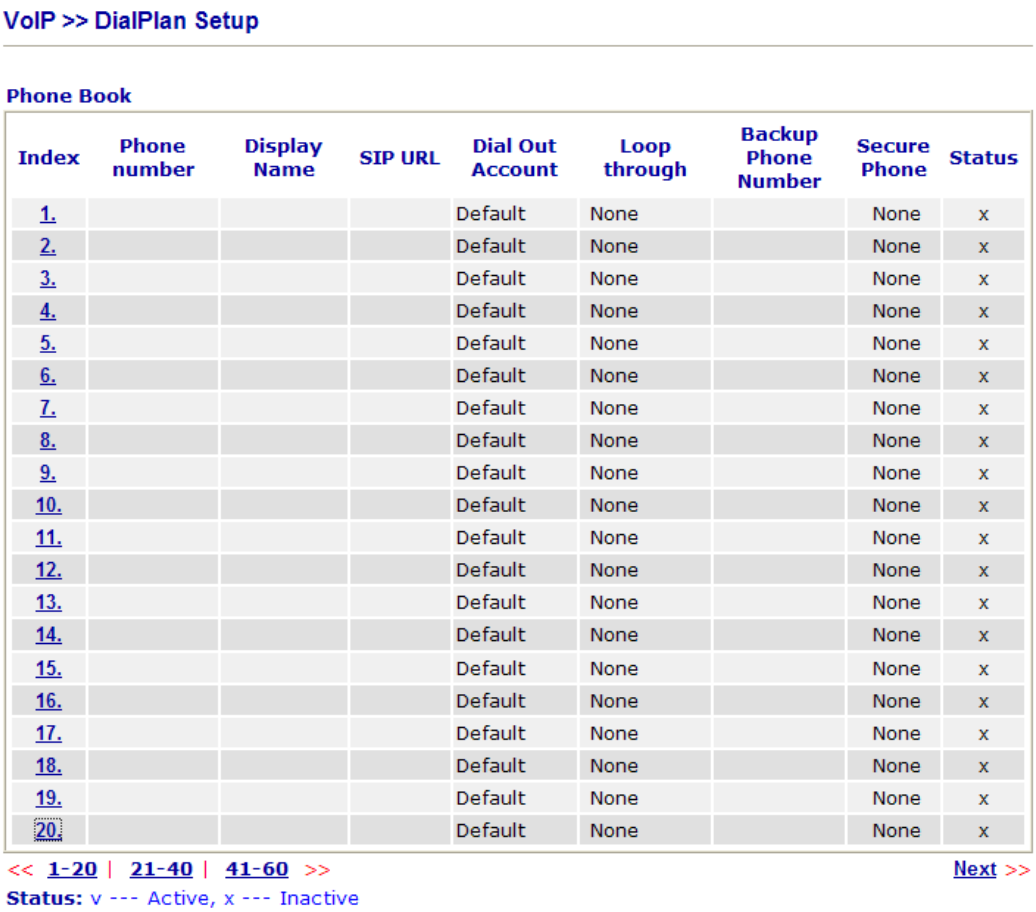
3.11.1 DialPlan

This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book** and **Digit Map** links on the page to access into next pages for dialplan settings.

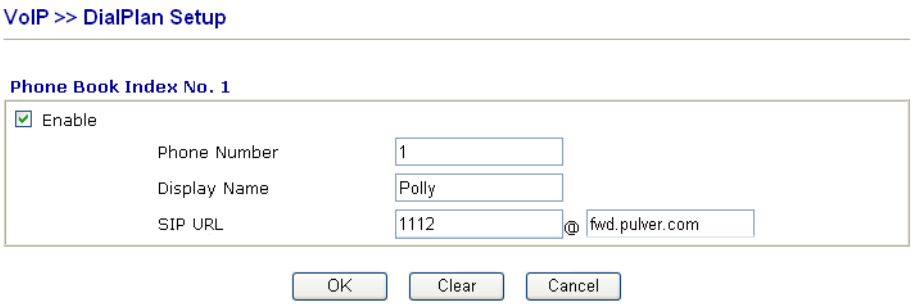


Phone Book

In this section, you can set your VoIP contacts in the “phonebook”. It can help you to make calls quickly and easily by using “speed-dial” **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members’ SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor 2820V for setting the phone book.

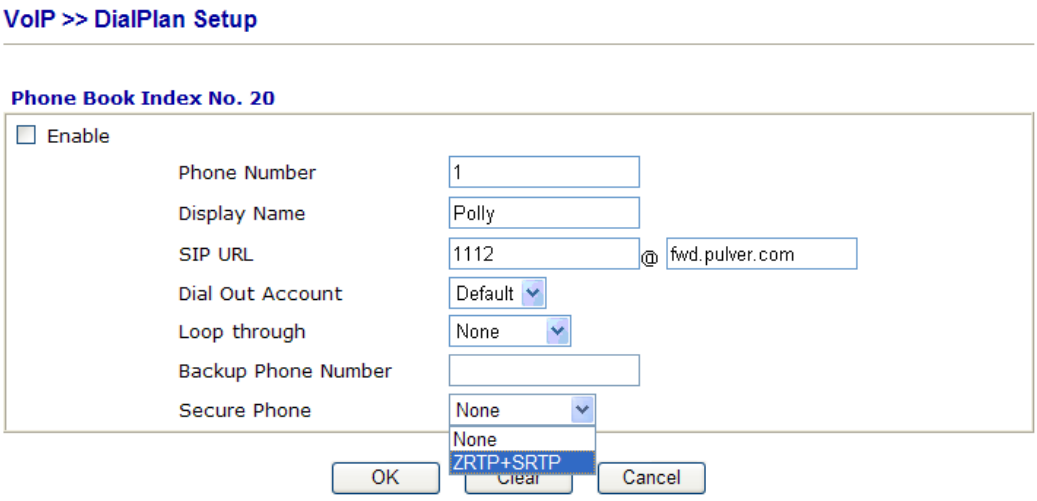


Click any index number to display the dial plan setup page.



Enable	Click this to enable this entry.
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits **0-9** and ***** .
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.
SIP URL	Enter your friend's SIP Address

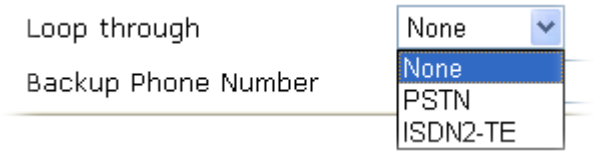
This page will differ for different models. Below is a sample page obtained from Vigor 2820VSn. The selection of **Loop through** and **Backup Phone Number** is only available for 2820VSn/2820Vn model.



Enable	Click this to enable this entry.
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits **0-9** and ***** .
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.
SIP URL	Enter your friend's SIP Address.
Dial Out Account	Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.

Loop through

For the model of Vigor 2820Vn, the selection should be as the following:



Backup Phone Number

When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number (PSTN number/ISDN number) for this VoIP phone setting.

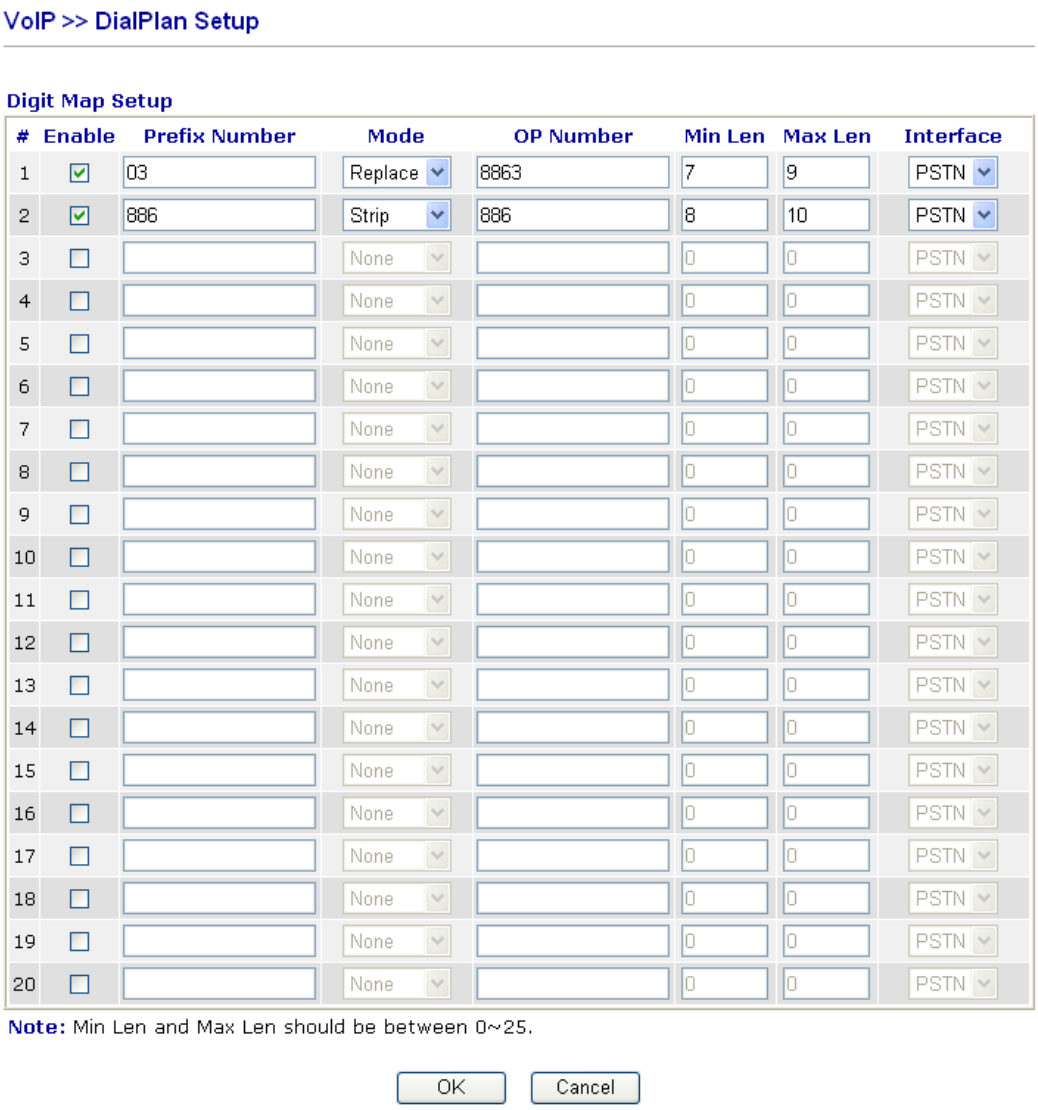
Secure Phone

ZRTP is a cryptographic key-agreement protocol to encrypt VoIP phone calls to ensure the phone security. It allows users to encrypt any Session Initiation Protocol (SIP) VoIP voice stream, as long as the peer side on the call is also using such protocol.
None - If the incoming or outgoing call matches the phone book entry with secure phone option set to "None", it means the call should be unprotected.
ZRTP+SRTP – If the incoming or outgoing call matches the phone book entry with secure phone option set to "ZRTP+SRTP", it means the call would be protected. A warning message will be played out if the call ends up unprotected.

Note: If the incoming or outgoing calls do not match any entry on the phonebook, the router will try to make the call "being protected". But, if the call ends up "unprotected"(e.g. peer side does not support ZRTP+SRTP), the router will not play out a warning message.

Digit Map

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.


VoIP >> DialPlan Setup
Digit Map Setup
Enable Prefix Number Mode OP Number Min Len Max Len Interface
1 03 Replace 8863 7 9 PSTN
2 886 Strip 886 8 10 PSTN
3 None 0 0 PSTN
4 None 0 0 PSTN
5 None 0 0 PSTN
6 None 0 0 PSTN
7 None 0 0 PSTN
8 None 0 0 PSTN
9 None 0 0 PSTN
10 None 0 0 PSTN
11 None 0 0 PSTN
12 None 0 0 PSTN
13 None 0 0 PSTN
14 None 0 0 PSTN
15 None 0 0 PSTN
16 None 0 0 PSTN
17 None 0 0 PSTN
18 None 0 0 PSTN
19 None 0 0 PSTN
20 None 0 0 PSTN
Note: Min Len and Max Len should be between 0~25.
OK
Cancel

Enable Check this box to invoke this setting.

Prefix Number The phone number set here is used to add, strip, or replace the OP number.

Mode

None - No action.
Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface.
Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of *886* will be deleted completely for the prefix number is set with *886*.
Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the

specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of “031111111” will be changed to “88631111111” and sent to SIP server.

Mode

OP Number The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.

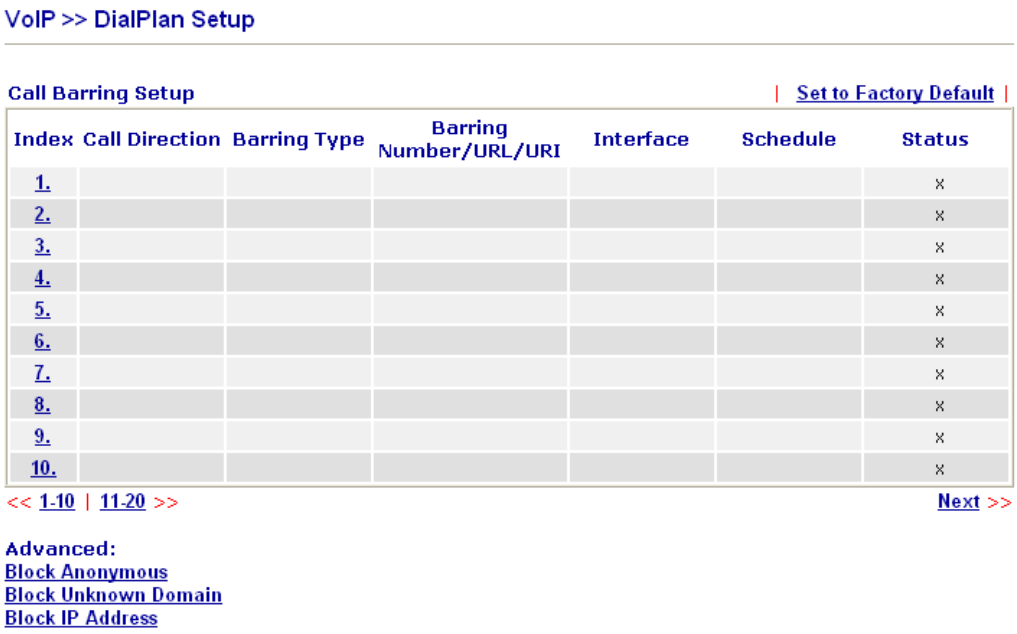
Min Len Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.

Max Len Set the maximum length of the dial number for applying the prefix number settings.

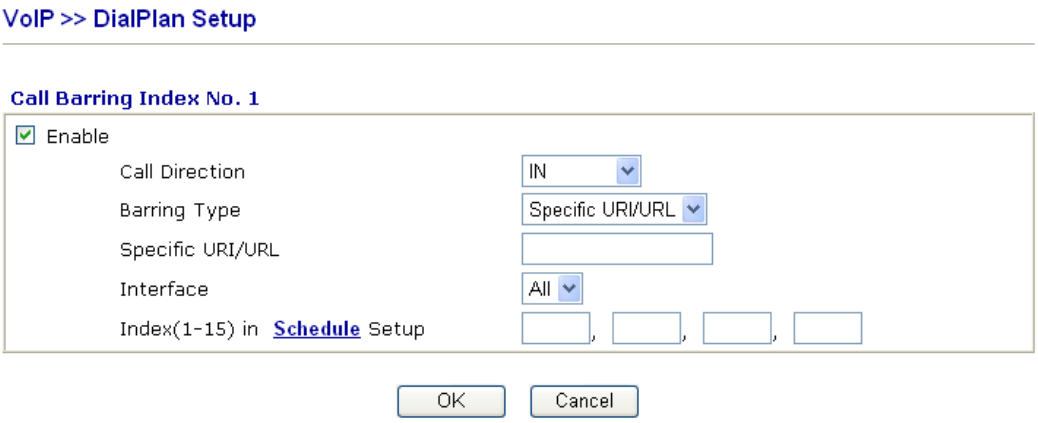
Interface Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available.

Call Barring

Call barring is used to block phone calls coming from the one that is not welcomed.

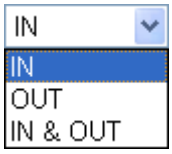


Click any index number to display the dial plan setup page.

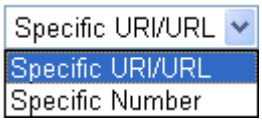


Enable Click this to enable this entry.

Call Direction Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.



Barring Type Determine the type of the VoIP phone call, URI/URL or number.



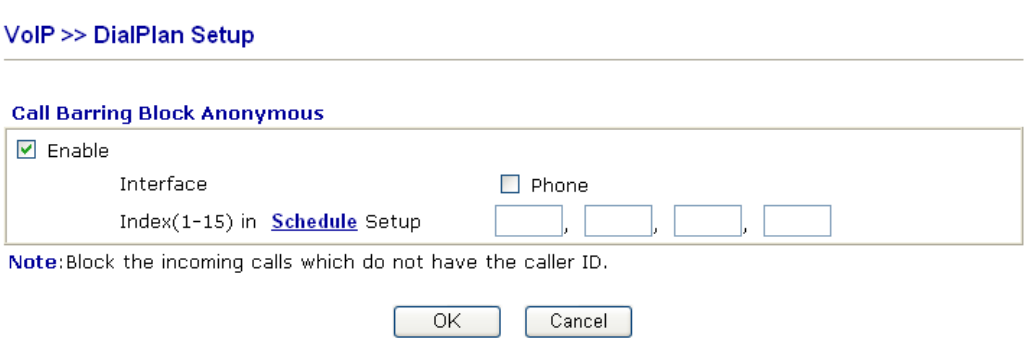
Specific URI/URL or Specific Number This field will be changed based on the type you selected for barring Type.

Interface **All** means all the phone calls will be blocked with such mechanism. **ISDN** means ISDN call will be blocked with such mechanism.

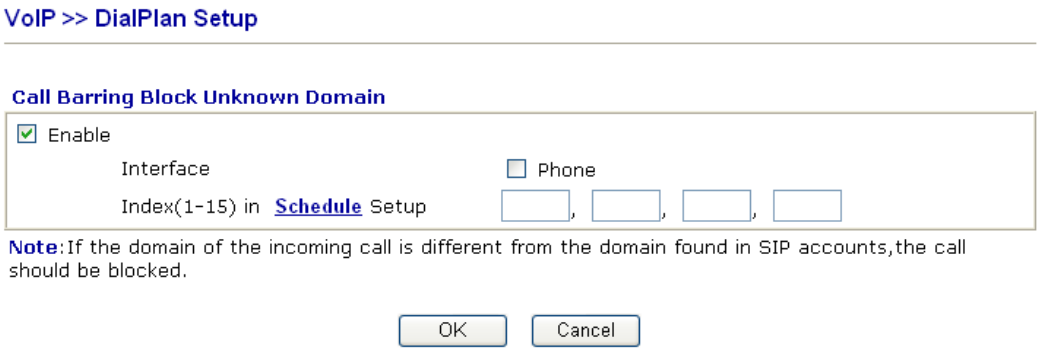
Index (1-15) in Schedule Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section **3.5.2 Schedule** for detailed configuration.

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

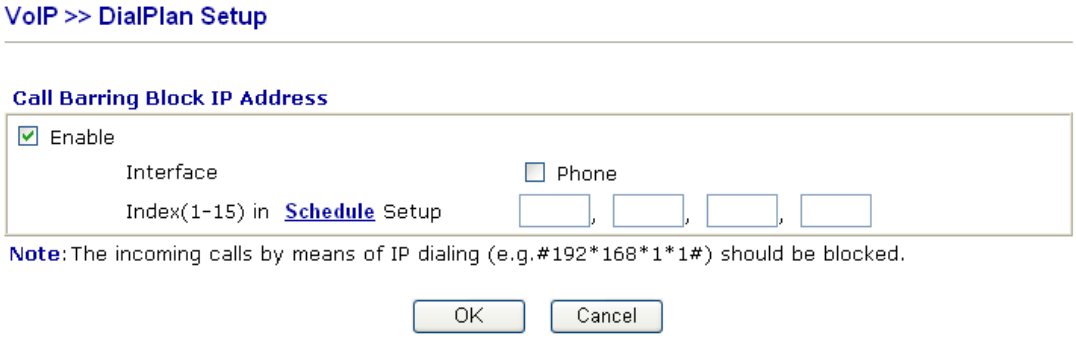
For **Block Anonymous –** this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.



For **Block Unknown Domain –** this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.

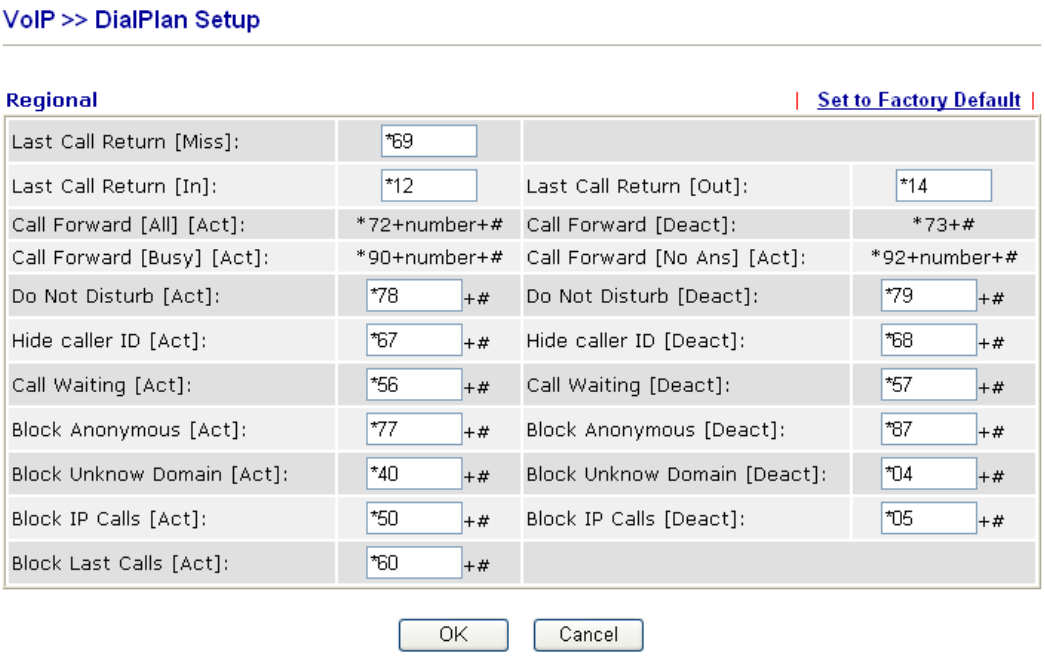

VoIP >> DialPlan Setup
Call Barring Block Unknown Domain
Enable
Interface
Phone
Index(1-15) in Schedule Setup
Note: If the domain of the incoming call is different from the domain found in SIP accounts, the call should be blocked.
OK
Cancel

For **Block IP Address –** this function can block incoming calls (through Phone port) coming from IP address. Such control also can be done based on preconfigured schedules.



Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You ***can change*** the number based on the region that the router is placed.


VoIP >> DialPlan Setup
Regional
Set to Factory Default
Last Call Return [Miss]: *69
Last Call Return [In]: *12
Last Call Return [Out]: *14
Call Forward [All] [Act]: *72+number+#
Call Forward [Deact]: *73+#
Call Forward [Busy] [Act]: *90+number+#
Call Forward [No Ans] [Act]: *92+number+#
Do Not Disturb [Act]: *78 +#
Do Not Disturb [Deact]: *79 +#
Hide caller ID [Act]: *67 +#
Hide caller ID [Deact]: *68 +#
Call Waiting [Act]: *56 +#
Call Waiting [Deact]: *57 +#
Block Anonymous [Act]: *77 +#
Block Anonymous [Deact]: *87 +#
Block Unknow Domain [Act]: *40 +#
Block Unknow Domain [Deact]: *04 +#
Block IP Calls [Act]: *50 +#
Block IP Calls [Deact]: *05 +#
Block Last Calls [Act]: *60 +#
OK
Cancel

Last Call Return [Miss] Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.

Last Call Return [In] You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.

Last Call Return [Out] Dial the number typed in this field to call the previous outgoing phone call again.

Call Forward [All][Act] Dial the number typed in this field to forward all the incoming calls to the specified place.

Call Forward [Deact] Dial the number typed in this field to release the call forward function.

Call Forward [Busy][Act] Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.

Call Forward [No Ans][Act] Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.

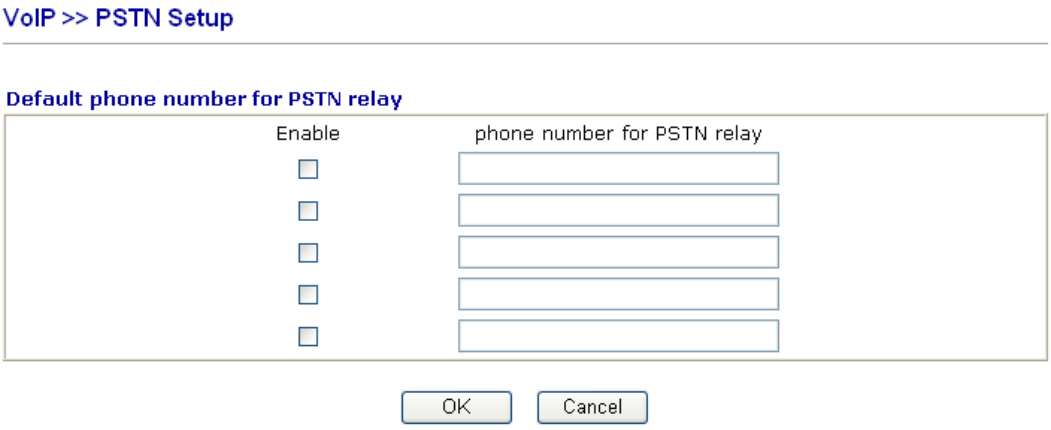
Do Not Disturb [Act] Dial the number typed in this field to invoke the function of DND.

Do Not Distrub [Deact] Dial the number typed in this field to release the DND function.

Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this filed to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

PSTN Setup

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Please type the number in the field of **phone number for PSTN relay**.



Then, check the **Enable** box to make the PSTN number available for dial whenever you need.

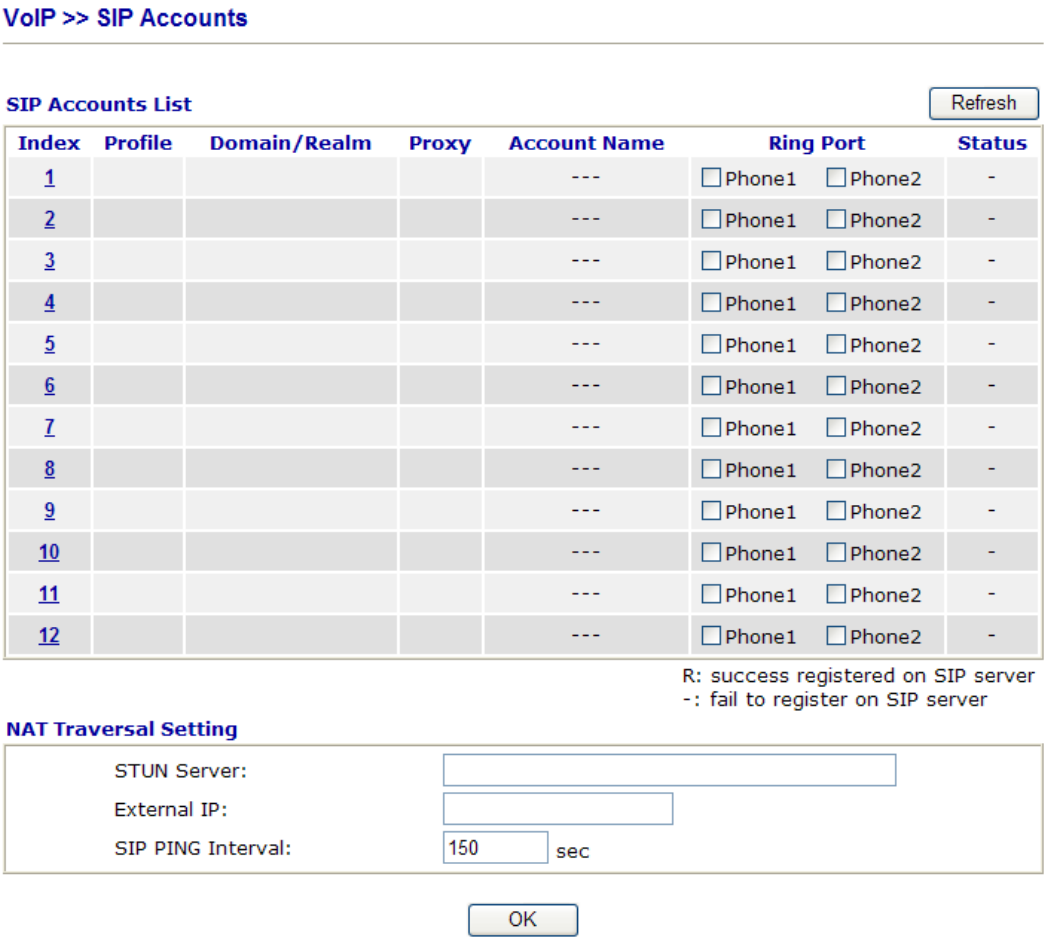
3.11.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar, Proxy,** and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name**

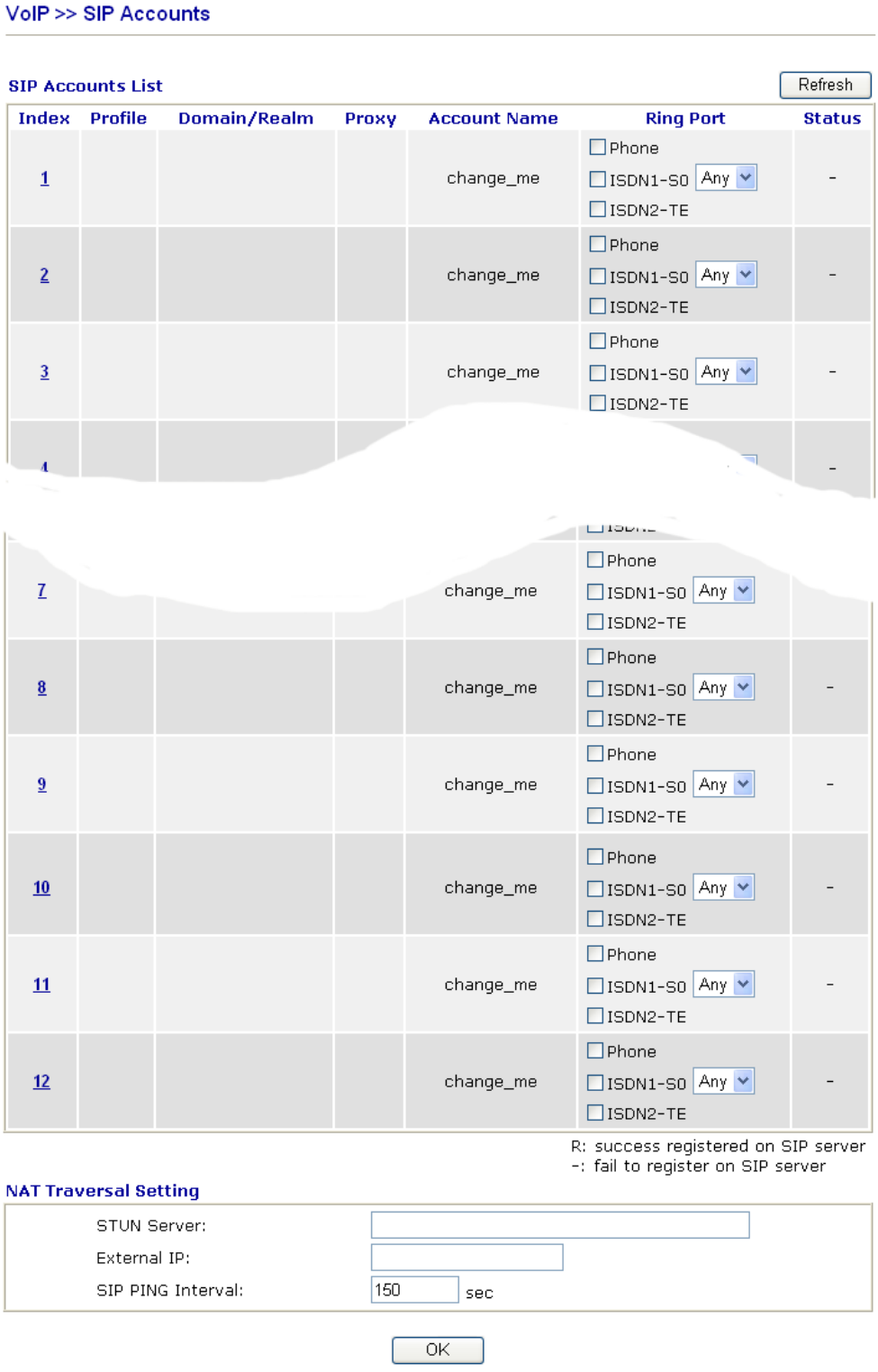
As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

Note: Selection items for **Ring Port** will differ according to the router you have.

For Vigor2820V/Vigor2820Vn models, you will see the following page:

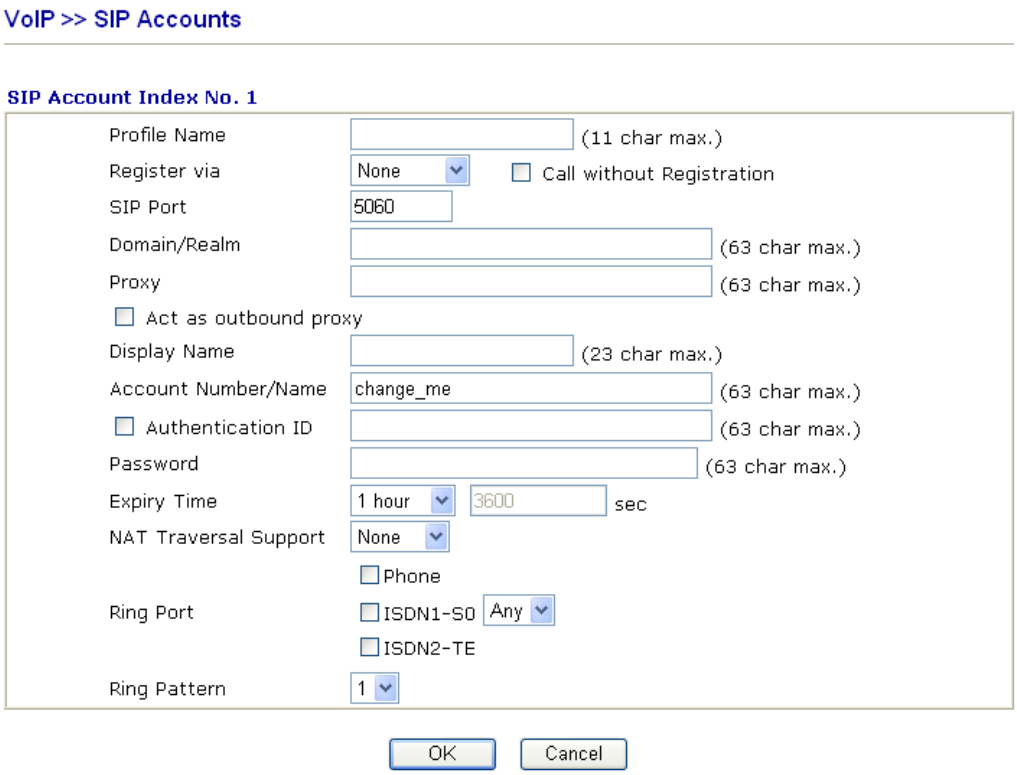

VoIP >> SIP Accounts
SIP Accounts List
Refresh
Index Profile Domain/Realm Proxy Account Name Ring Port Status
1 --- Phone1 Phone2 -
2 --- Phone1 Phone2 -
3 --- Phone1 Phone2 -
4 --- Phone1 Phone2 -
5 --- Phone1 Phone2 -
6 --- Phone1 Phone2 -
7 --- Phone1 Phone2 -
8 --- Phone1 Phone2 -
9 --- Phone1 Phone2 -
10 --- Phone1 Phone2 -
11 --- Phone1 Phone2 -
12 --- Phone1 Phone2 -
R: success registered on SIP server
-: fail to register on SIP server
NAT Traversal Setting
STUN Server:
External IP:
SIP PING Interval:
150
sec
OK

For Vigor2820VS/Vigor2820VSn models, you will see the following page:



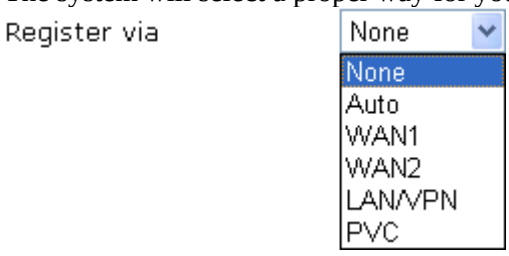
Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.

Account Name	Display the account name of SIP address before @.
Ring Port	Specify which port will ring when receiving a phone call. Set Phone, ISDN1-S0 or ISDN-TE as the default ring port for the SIP account. If you choose Phone or ISDN1-S0, the ISDN2-TE selection will be dimmed, vice versa. There are ten internal lines with numbers (30 – 39) offered for **ISDN-S0**. You can specify any one of them as ring port for specified SIP account. By the way, ISDN-S0 can be used by mapping with MSN numbers.
STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
Status	Show the status for the corresponding SIP account. **R** means such account is registered on SIP server successfully. **–** means the account is failed to register on SIP server.



Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field.
Register via	If you want to make VoIP call without register personal information, please choose **None** and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of **Call without Registration**. Choosing **Auto** is recommended.

The system will select a proper way for your VoIP call.



SIP Port Set the port number for sending/receiving SIP message for building a session. The default value is **5060.** Your peer must set the same value in his/her Registrar.

Domain/Realm Set the domain name or IP address of the SIP Registrar server.

Proxy Set domain name or IP address of SIP proxy server. By the time you can type **:port number** after the domain name to specify that port as the destination of data transmission (e.g., **nat.draytel.org:5065**)

Act as Outbound Proxy Check this box to make the proxy acting as outbound proxy.

Display Name The caller-ID that you want to be displayed on your friend's screen.

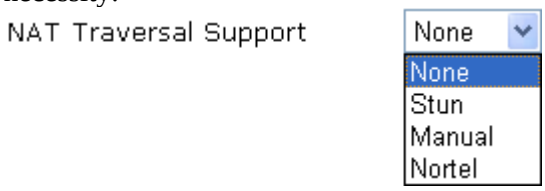
Account Number/Name Enter your account name of SIP Address, e.g. every text before @.

Authentication ID Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.

Password The password provided to you when you registered with a SIP service.

Expiry Time The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.

NAT Traversal Support If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.

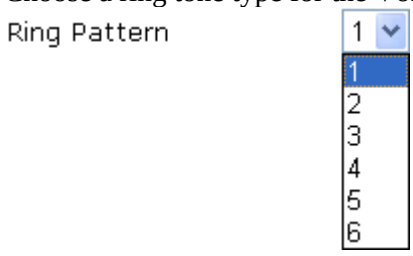


None – Disable this function.
Stun – Choose this option if there is Stun server provided for your router.
Manual – Choose this option if you want to specify an external IP address as the NAT transversal support.
Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option.

Ring Port Set Phone, ISDN1-S0 or ISDN-TE as the default ring port for this SIP account. If you choose Phone or ISDN1-S0, the ISDN2-TE selection will be dimmed, vice versa. There are ten internal lines with numbers (30 – 39) offered for **ISDN-S0**. You

can specify one of them or choose **Any** as ring port for specified SIP account. By the way, ISDN-S0 can be used by mapping with MSN numbers.

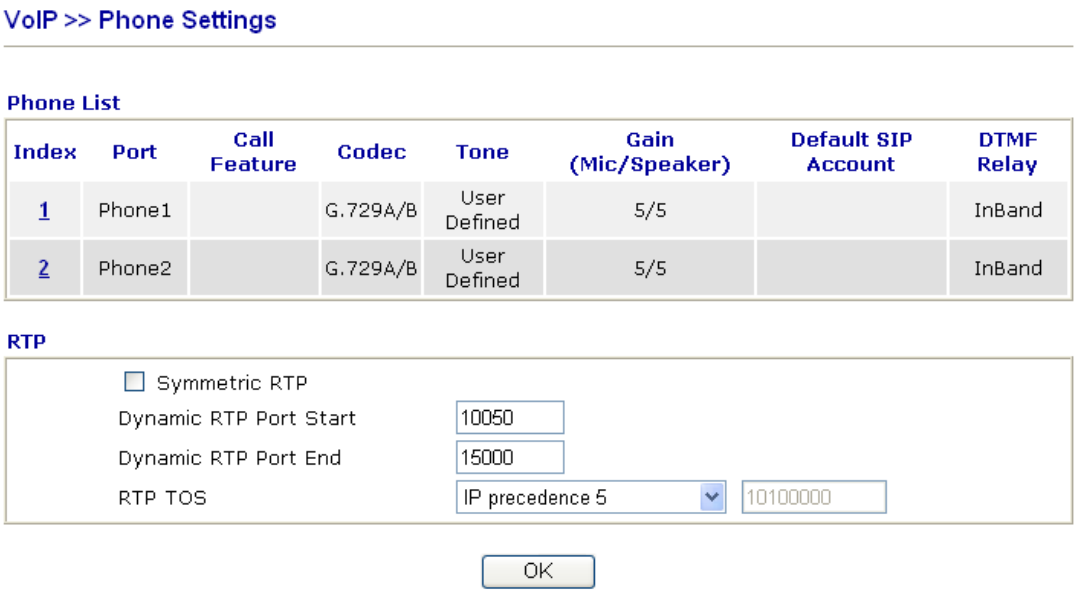
Ring Pattern Choose a ring tone type for the VoIP phone call.



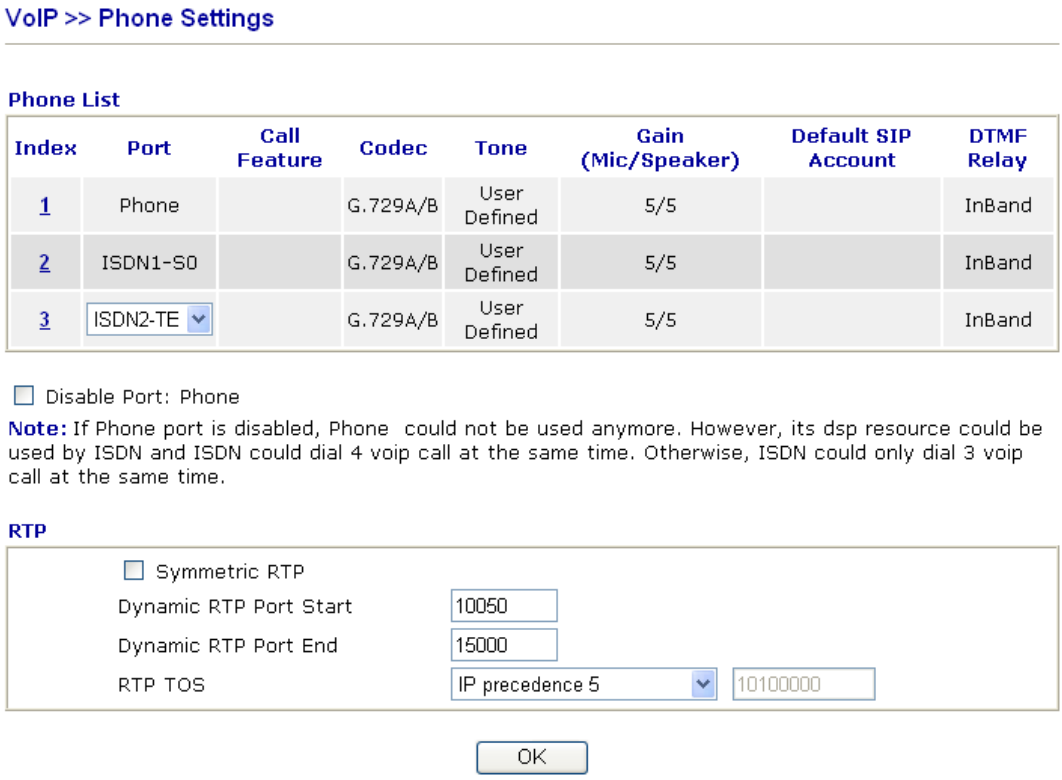
3.11.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

For Vigor2820V/Vigor2820Vn models, you will see the following page:



For Vigor2820VS/Vigor2820VSn models, you will see the following page:



Phone List

Port – For Vigor2820V/Vigor2820Vn, there are two phone ports provided here for you to configure. However, for Vigor2820VS/Vigor2820VSn, there are three phone ports provided here for you to configure. Two (Index 1 to 2) are fixed and one (Index 3) is configurable. **Phone1/Phone2/Phone** allow you to set general settings for PSTN phones. **ISDN1-S0** and **ISDN2-TE** allow you to set common settings for ISDN network connection. ISDN2 port is configurable. Please use the drop down list to choose **ISDN2-TE** for Internet connection or choose **ISDN2-S0** (ISDN intern) for ISDN phone. In addition, you can connect six phones to this router in certain case. Please refer to **Section 4-1** for detailed information of ISDN phone/network connection.
If you want to enable function of ISDN On-Net/Off-Net, you have to choose ISDN2-TE.
Call Feature – A brief description for call feature will be shown in this field for your reference.
Codec – The default Codec setting for each port will be shown in this field for your reference. You can click the number below the Index field to change it for each phone port.
Tone - Display the tone settings that configured in the advanced settings page of Phone Index.
Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index.
Default SIP Account – "draytel_1" is the default SIP account. You can click the number below the Index field to change SIP account for each phone port.
DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index.

Disable Port

The router can support up to 4 VoIP calls simultaneously. In general, only 3 VoIP calls can be dialed through ISDN at the same time. If you want to use four ISDN channels, you have to check this box. When the Phone port is disabled, it could not be used anymore.

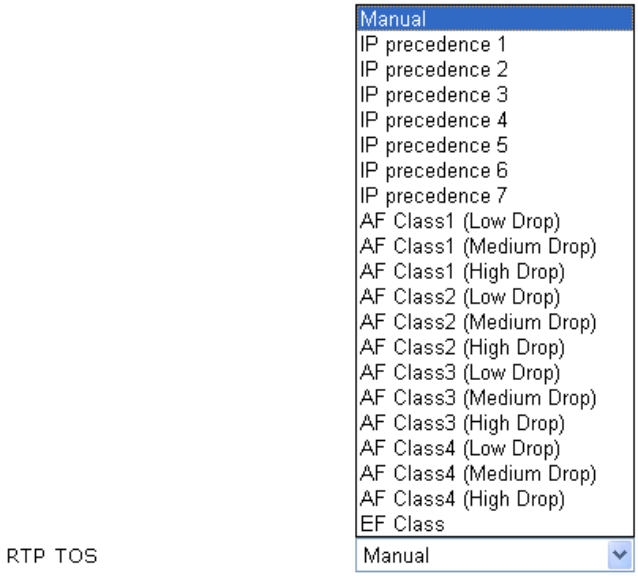
RTP

Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem.

Dynamic RTP Port Start - Specifies the start port for RTP stream. The default value is 10050.

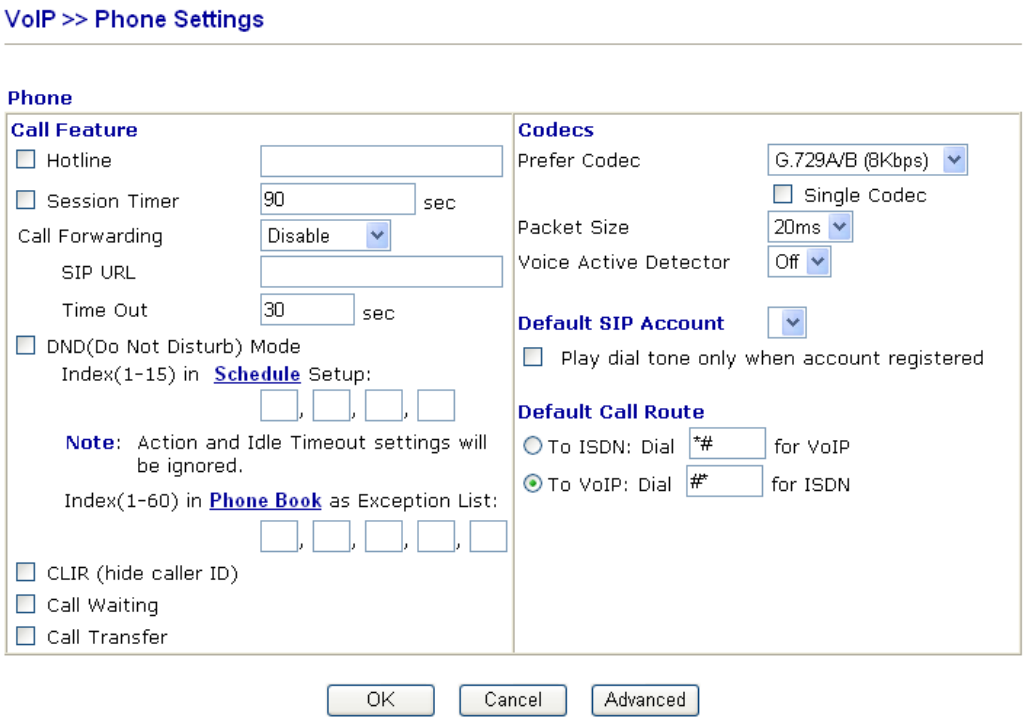
Dynamic RTP Port End - Specifies the end port for RTP stream. The default value is 15000.

RTP TOS – It decides the level of VoIP package. Use the drop down list to choose any one of them.



Detailed Settings for Phone Port

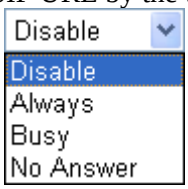
Click the number link for Phone port, you can access into the following page for configuring Phone settings.



Hotline — Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

Session Timer — Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.

Call Forwarding — There are four options for you to choose. **Disable** is to close call forwarding function. **Always** means all the incoming calls will be forwarded into SIP URL without any reason. **Busy** means the incoming calls will be forwarded into SIP URL only when the local system is busy. **No Answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.



SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.
Time Out – Set the time out for the call forwarding. The default setting is 30 sec.

DND (Do Not Disturb) mode — Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.

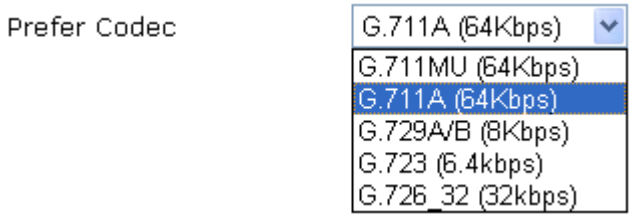
Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section **3.8.2 Schedule** for detailed configuration.
Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section **3.11.1 DialPlan – Phone Book** for detailed configuration.

CLIR (hide caller ID) Check this box to hide the caller ID on the display panel of the phone set.

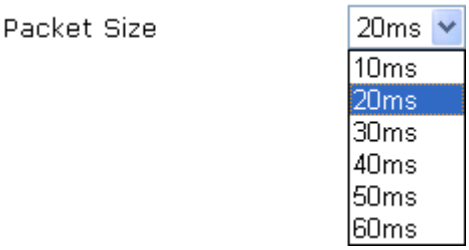
Call Waiting Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.

Call Transfer Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.

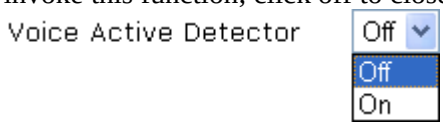
Prefer Codec Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.
If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.



Single Codec – If the box is checked, only the selected Codec will be applied.
Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.



Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.



Default SIP Account

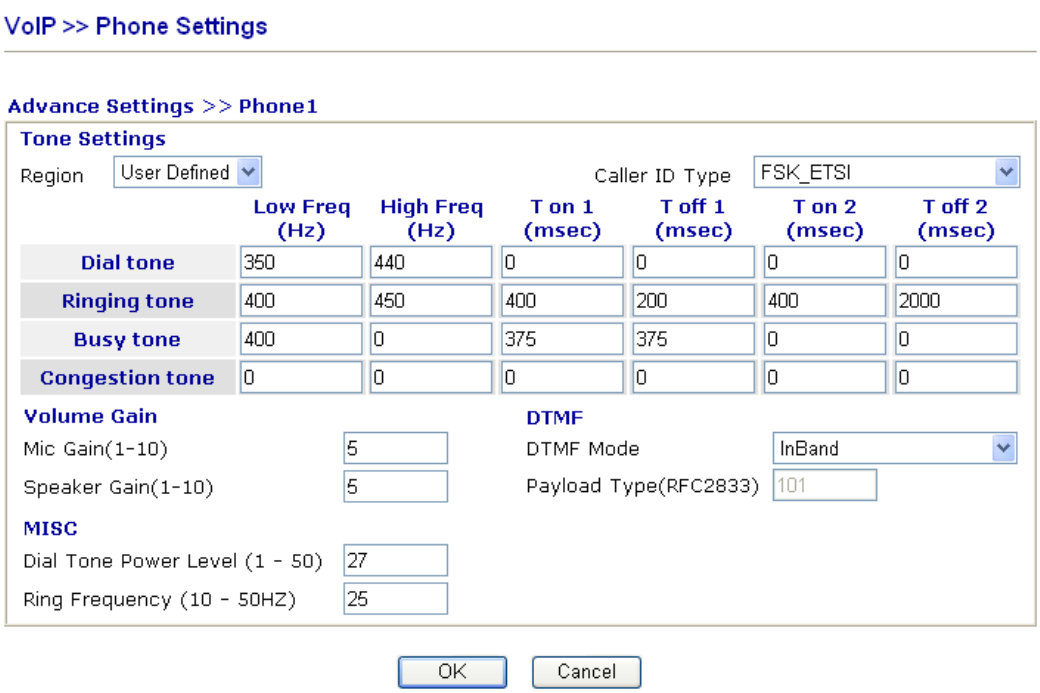
You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

Play dial tone only when account registered - Check this box to invoke the function.

Default Call Route

It determines the default direction for the call route of the router. Such feature is available for **Vigor2820VS** and **Vigor2820VSn**.
To ISDN (for VoIP) - The router is set by using ISDN call. To change ISDN call into VoIP call, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9.
To VoIP (for ISDN) - The router is set by using VoIP call. To change VoIP call into ISDN call, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.



Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.

Volume Gain

Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.

MISC

Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.

Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.

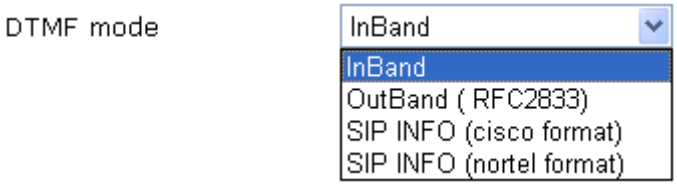
DTMF

DTMF Mode – There are four DTMF modes for you to choose.

InBand **-** Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone

OutBand **-** Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

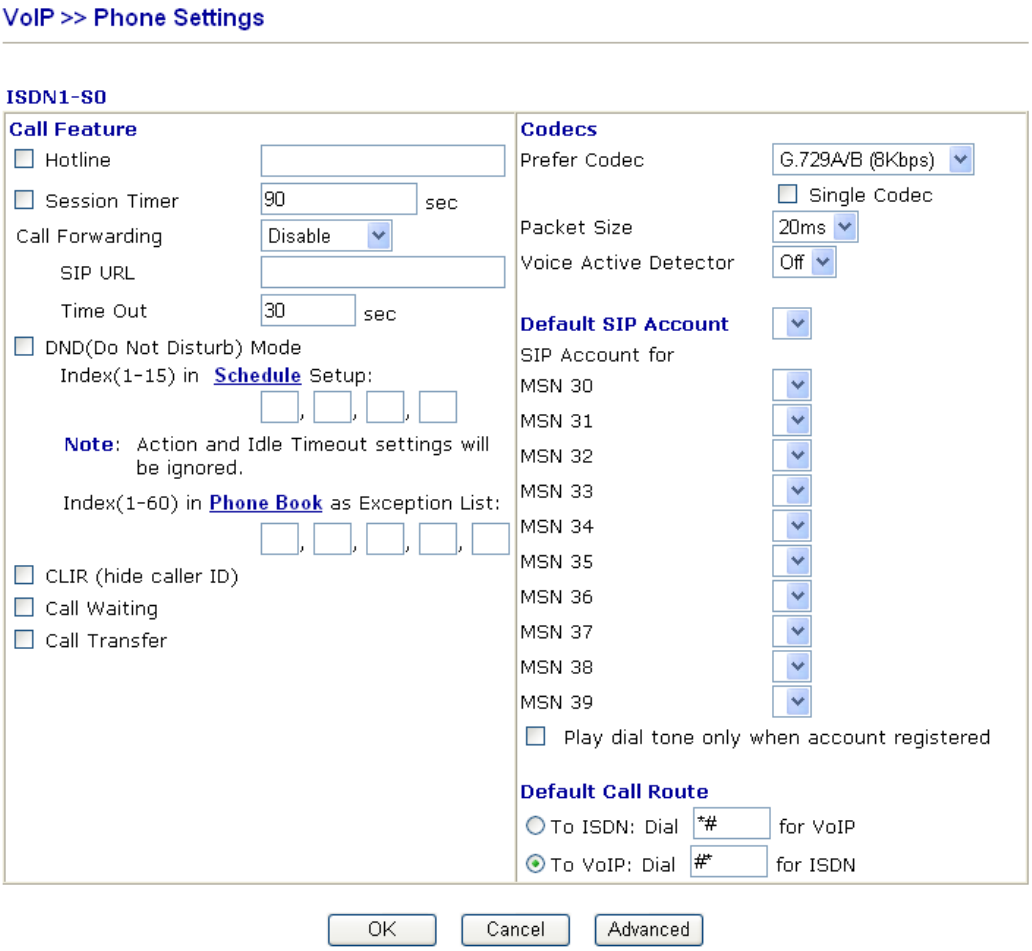
SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.



Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

Detailed Settings for ISDN1-S0 Port

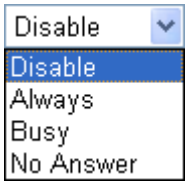
Click the number link of Index 2 (ISDN1-S0), you can access into the following page for configuring Phone settings.



Hotline — Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

Session Timer — Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.

Call Forwarding — There are four options for you to choose. **Disable** is to close call forwarding function. **Always** means all the incoming calls will be forwarded into SIP URL without any reason. **Busy** means the incoming calls will be forwarded into SIP URL only when the local system is busy. **No answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.



SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or

abc@iptel.org) as the site for call forwarded.
Time Out – Set the time out for the call forwarding. The default setting is 30 sec.

DND (Do Not Disturb) mode

Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.

Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section **3.8.2 Schedule** for detailed configuration.
Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section **3.11.1 DialPlan – Phone Book** for detailed configuration.

CLIR (hide caller ID)

Check this box to hide the caller ID on the display panel of the phone set.

Call Waiting

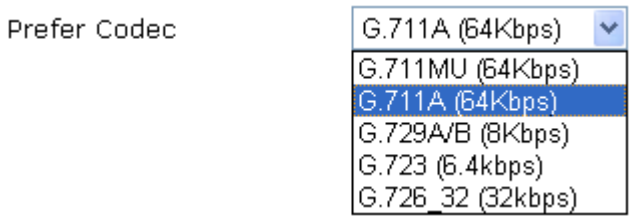
Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.

Call Transfer

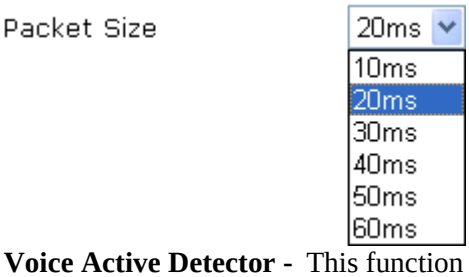
Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.

Prefer Codec

Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.
If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.

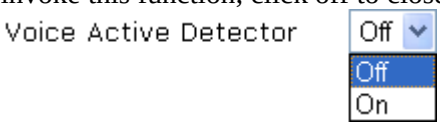


Single Codec – If the box is checked, only the selected Codec will be applied.
Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.



Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to

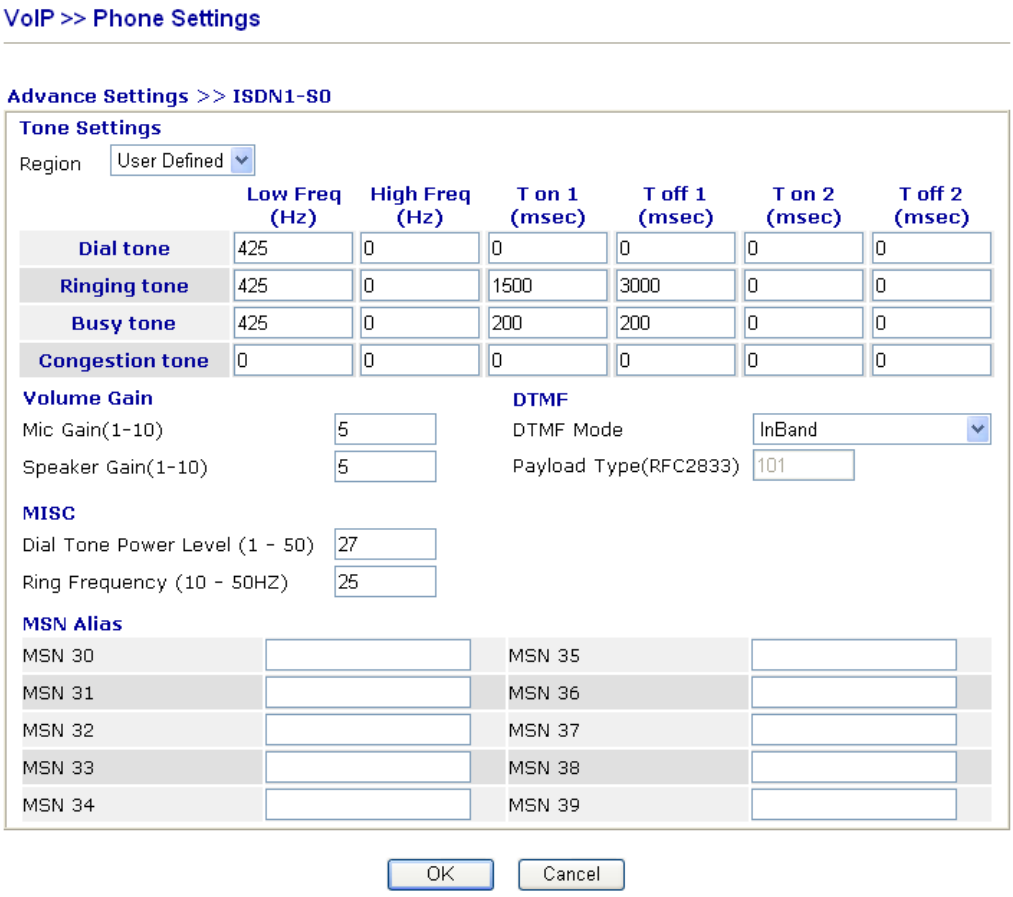
invoke this function; click off to close the function.



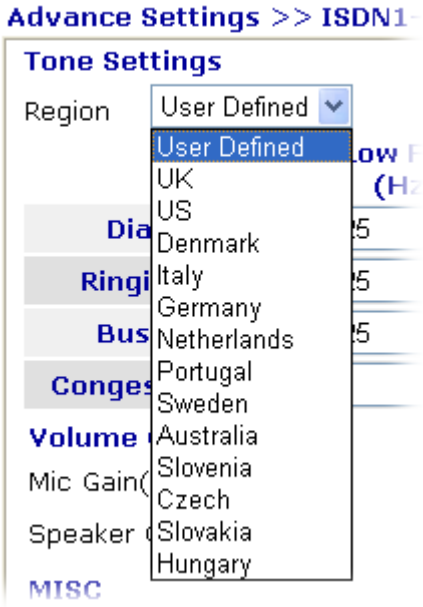
Default SIP Account — You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting. ISDN-S0 port can pick up multiple incoming calls simultaneously. Therefore different phone sets (MSN30 to MSN39) can use different SIP accounts to call out through this port.
Play dial tone only when account registered - Check this box to invoke the function.

Default Call Route — It determines the default direction for the call route of the router.
To ISDN (for VoIP) - The router is set by using ISDN call. To change ISDN call into VoIP call, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9.
To VoIP (for ISDN) - The router is set by using VoIP call. To change VoIP call into ISDN call, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC, DTMF mode and MSN number. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.



Region Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.



Also, you can specify each field for your necessity. It is

recommended for you to use the default settings for VoIP communication.

Volume Gain

Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.

MISC

Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.

Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.

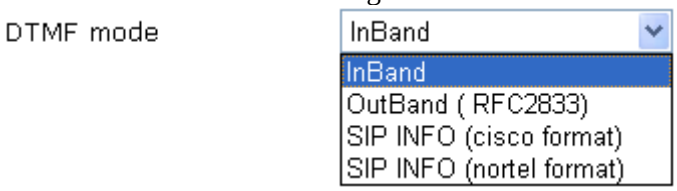
DTMF

DTMF Mode – There are four DTMF modes for you to choose.

InBand **-** Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone

OutBand **-** Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

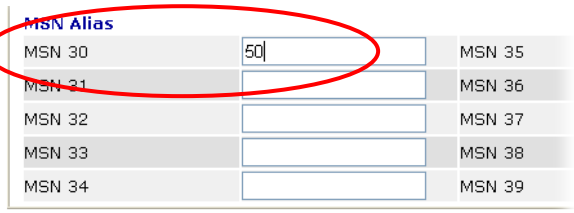
SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.



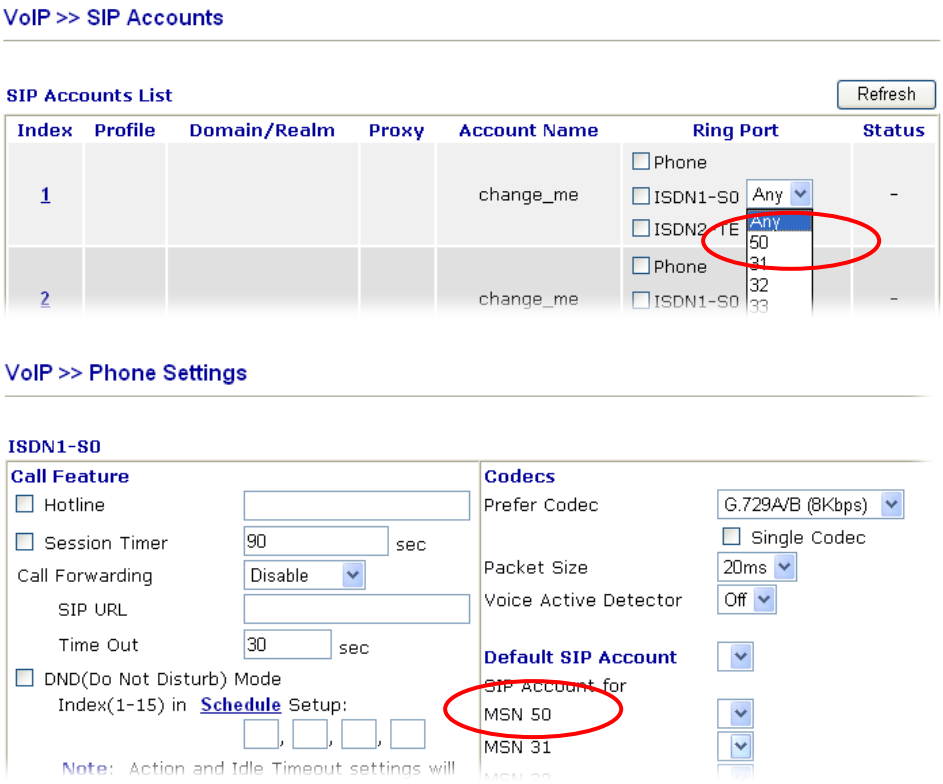
Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

MSN Alias

You can modify the MSN number (default values are set from 30 – 39) with any number you desire. For example, type 50 in the box of MSN 30.

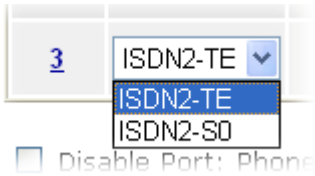


Later you will find MSN 30 has been replaced with MSN50 in all related pages. See the following figures for examples (pages of **VoIP>>SIP Accounts** and **VoIP>>Phone Settings**).

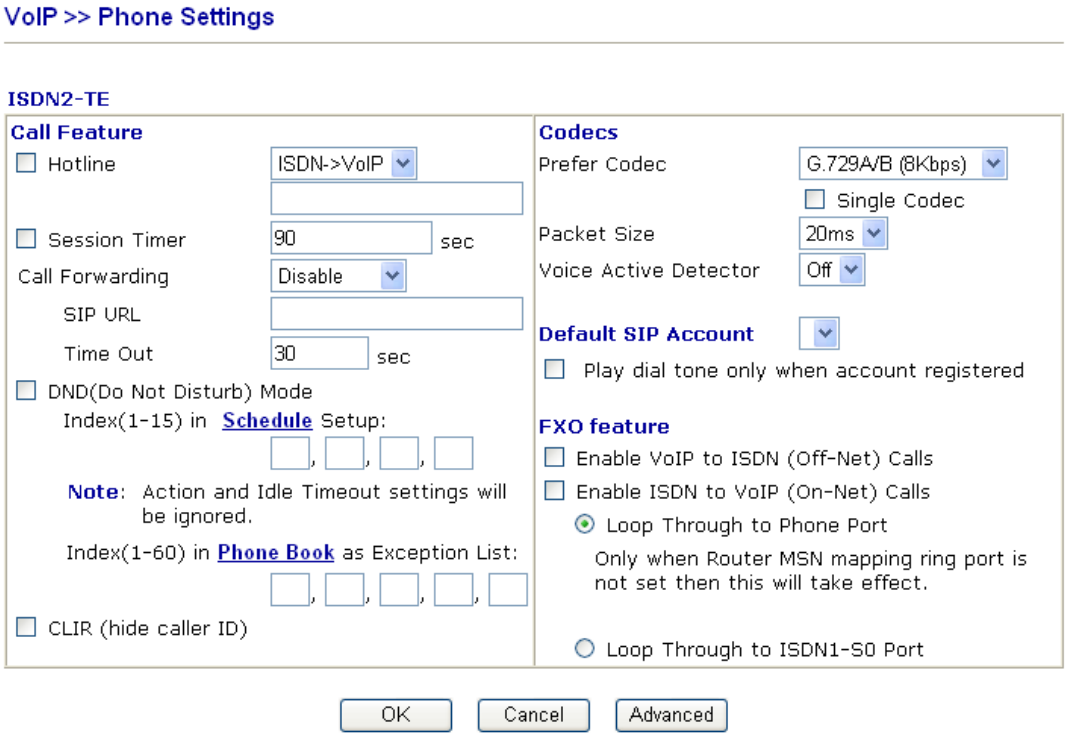


Detailed Settings for ISDN2-TE Port (Available for *VSn* model only)

Vigor2820VSn allows users to switch the function of ISDN2 port between TE or S0 mode. Please use the drop down list to choose the one you want.



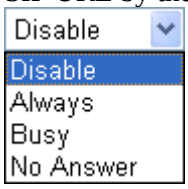
If you choose ISDN2-S0, please refer to Detailed Settings for Phone1, Phone2, ISDN1-S0 for the configuration. However, if you choose ISDN-TE and click the number link for that port, you will see the following page.



Hotline — Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

Session Timer — Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.

Call Forwarding — There are four options for you to choose. **Disable** is to close call forwarding function. **Always** means all the incoming calls will be forwarded into SIP URL without any reason. **Busy** means the incoming calls will be forwarded into SIP URL only when the local system is busy. **No answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.



SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.
Time Out – Set the time out for the call forwarding. The default setting is 30 sec.

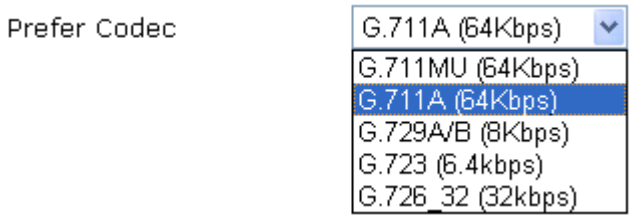
DND (Do Not Disturb) mode — Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.

Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section **3.8.2 Schedule** for detailed configuration.
Index (1-60) in Phone Book - Enter the index of phone book

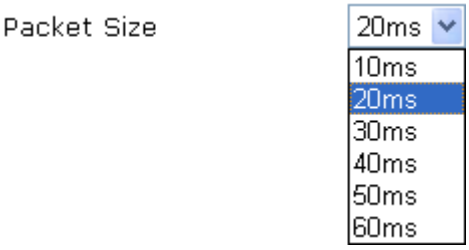
profiles. Refer to section **3.11.1 DialPlan – Phone Book** for detailed configuration.

CLIR (hide caller ID) Check this box to hide the caller ID on the display panel of the phone set.

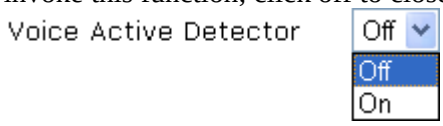
Prefer Codec Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.
If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.



Single Codec – If the box is checked, only the selected Codec will be applied.
Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.



Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

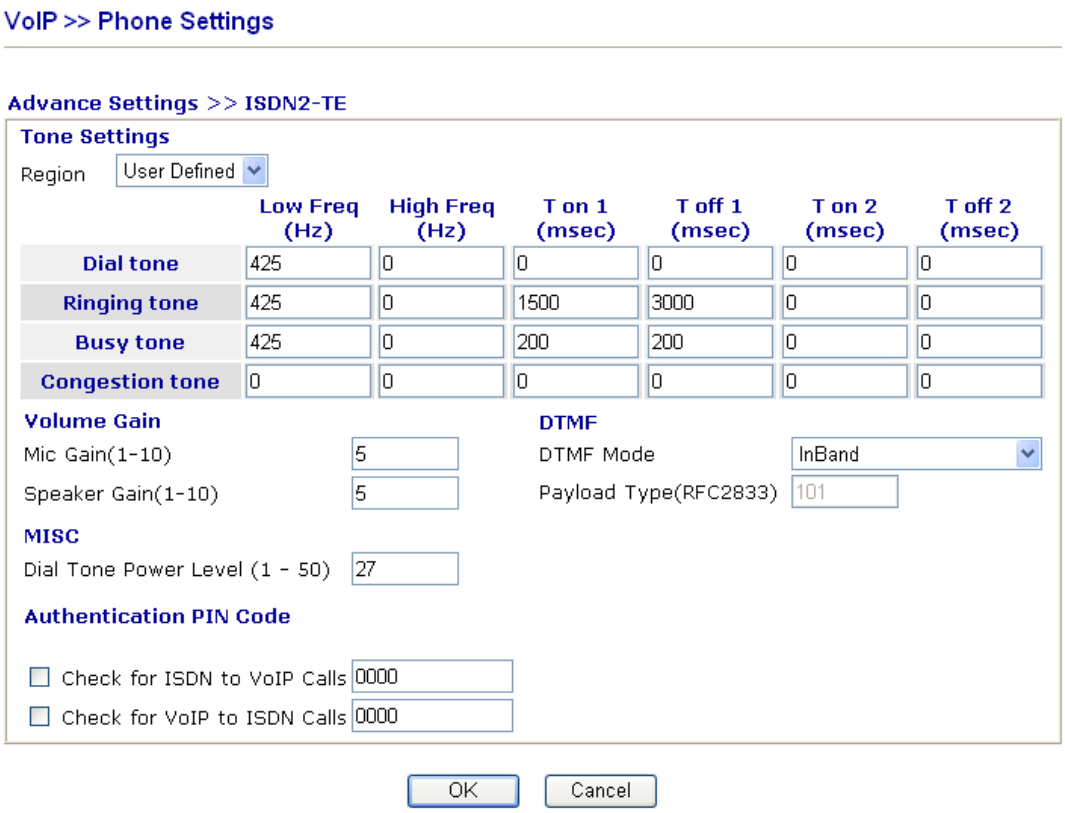


Default SIP Account You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.
Play dial tone only when account registered - Check this box to invoke the function.

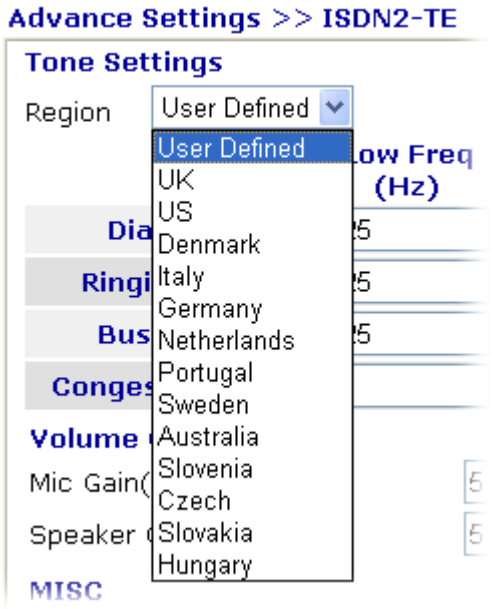
FXO Feature **Enable ISDN to VoIP (On-Net) Calls** – Check this box to make all the outgoing calls from ISDN line to be forwarded to receivers by Internet.
Enable VoIP to ISDN (Off-Net) Calls –Check this box to make all the incoming calls coming from Internet to be forwarded to receivers by ISDN line.
Loop Through to Phone Port – Choose this radio button to make all the calls controlled by traditional PSTN phone. It will tack effect only if MSN mapping ring port is not configured.

Loop Through to ISDN1-S0 Port – Choose this radio button to make all the calls controlled by ISDN line.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.



Region Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.



Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.

Volume Gain

Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.

MISC

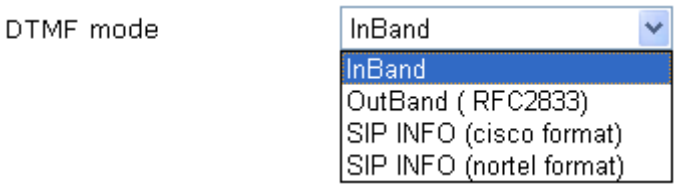
Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.

Authentication PIN Code

Check for ISDN to VoIP Calls – Set a pin code for the router to authenticate which one is allowed to dial ISDN to VoIP call. The figure that you can type in this field is limited from three to eight with digits from zero to nine.
Check for VoIP to ISDN Calls - Set a pin code for the router to authenticate which one is allowed to dial VoIP to ISDN call. The figure that you can type in this field is limited from three to eight with digits from zero to nine.

DTMP

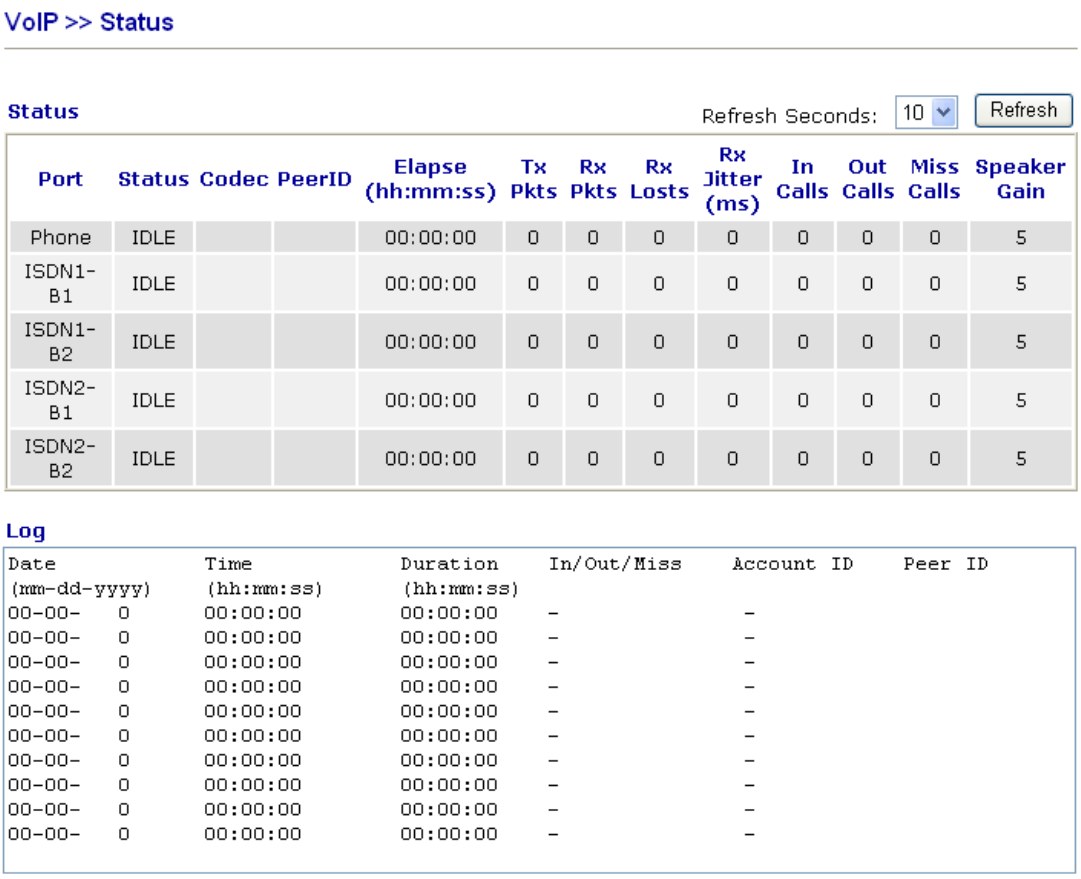
DTMF mode – There are four selections provided here:
InBand: Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone
OutBand: Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.
SIP INFO: Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.



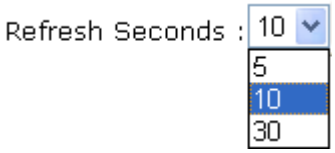
Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

3.11.4 Status

From this page, you can find codec, connection and other important call status for each port.



Refresh Seconds Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.



Port It shows current connection status for Phone(s) and ISDN ports.

Status It shows the VoIP connection status.
IDLE - Indicates that the VoIP function is idle.
HANG_UP - Indicates that the connection is not established (busy tone).
CONNECTING - Indicates that the user is calling out.
WAIT_ANS - Indicates that a connection is launched and

	waiting for remote user's answer. **ALERTING -** Indicates that a call is coming. **ACTIVE-**Indicates that the VoIP connection is launched.
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).
Elapse	The format is represented as hours:minutes:seconds.
Tx Pkts	Total number of transmitted voice packets during this connection session.
Rx Pkts	Total number of received voice packets during this connection session.
Rx Losts	Total number of lost packets during this connection session.
Rx Jitter	The jitter of received voice packets.
In Calls	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

3.12 ISDN

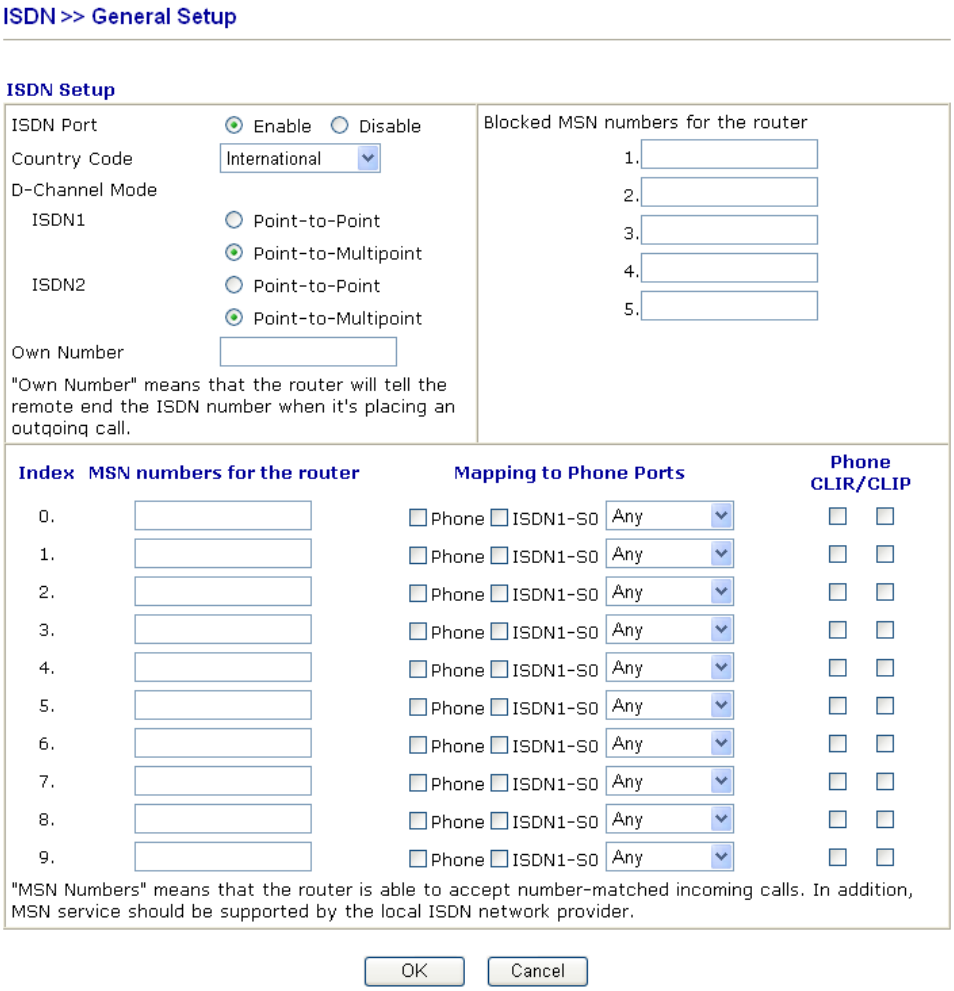
3.12.1 Basic Concept

ISDN means integrated services digital network that is an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.

Below shows the menu items for ISDN.

3.12.2 General Settings

This web page allows you to enable ISDN function.

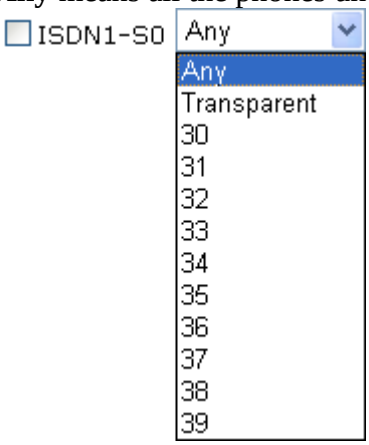


ISDN Port	Click **Enable** to open the ISDN port and **Disable** to close it.
Country Code	For proper operation on your local ISDN network, you should choose the correct country code.
D-Channel Mode	It allows you to configure ISDN layer2 protocol as: **Point-to-Point** - Configure ISDN port to use static TEI (Terminal Endpoint Identifier). **Point-to-Multipoint** - Configure ISDN port to use Dynamic TEI.
Own Number	Enter your ISDN number that you got from ISDN service provider (To have such number, you have offer your request from ISDN service provider first). Every outgoing call will carry the number to the receiver.
Blocked MSN Numbers for the router	Enter the specified MSN number into the fields to prevent the router from dialing the specific MSN number
MSN Numbers for the Router	MSN Numbers mean that the router is able to accept only number-matched incoming calls. In addition, local ISDN network provider should support MSN services. The router provides ten fields for MSN numbers. Note that MSN service must be acquired from your local telecom operators. By

default, MSN function is disabled. If you leave the fields blank, all incoming calls will be accepted without number matching.
1-10 fields – Fill in the portion that is different with the own number.
For example, the own number is **1234567** and MSN numbers are **1234*50***, **1234*17*** and **1234*82*** respectively. You can type in **1234567** in the filed of own number. Fill in **50**, **17** and **67** on the fields of 1, 2 and 3 one by one without typing 12345.

Mapping to Phone Ports

For loop through phone calls, you can assign Phone or/and ISDN1-S0 as ring ports if incoming calls correspond with settings on MSN number field.
There are ten internal lines (30-39) under ISDN1-S0 for you to configure as dedicated line. You can setup your ISDN phone with one of these 10 different internal MSN numbers. **Transparent** means MSN on TE port can connect to NT port without limitation on the number among 30 ~ 39. **Any** means all the phones under ISDN1-S0 would ring.



If you choose **Any** as ISDN-S0 port, when the router receives the incoming phone call with certain number for reaching ISDN-S0, all the phone sets connected to ISDN-S0 will ring at the same time.

Phone CLIR/CLIP

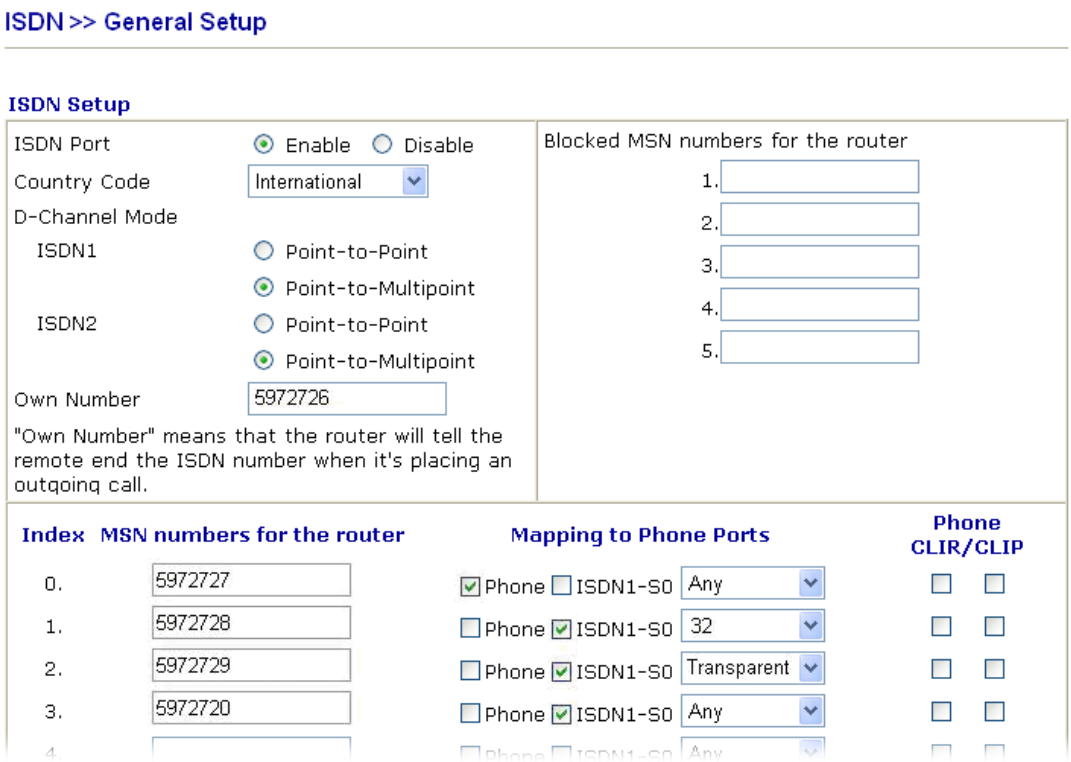
CLIR means “Calling Line Identification Restriction”. If you choose this item, we will not let remote side see your phone number. Such function depends on environment that ISP offers to you. Usually, hidden telephone number is not permitted under many real circumstances.

CLIP means “Calling Line Identification Presentation”. Usually the router will send "Own Number" to the remote side. However **Own number** will restrict the router displaying only one number on remote side. Vigor2820 series can connect up to 6
phones at the same time. Therefore, if **CLIP** is selected, the **external MSN numbers that you setup will be displayed to remote side**.

Application Example

You got ISDN numbers with ***5972720~5972729*** from your ISP, and you try to connect ISDN-TE port to ISDN network. Please refer to the following configuration.

Open **ISDN>> General Setup** and set as the following:



When remote user calls you by dialing ***5972727***, the router will make Phone port ringing.

When remote user calls you by dialing ***5972728***, the router will make ISDN phone under ISDN1-S0 port and configured with internal MSN number 32 ringing.

When remote user calls you by dialing ***5972729***, the router will make ISDN phones under ISDN1-S0 port and configured with internal MSN number ***5972729*** ringing.

When remote user calls you by dialing ***5972720***, the router will make all of ISDN phones under ISDN1-S0 port ringing.

When remote user calls you by dialing ***5972722***, the router will make no phone ringing for the number is not specified in such page.

If you use Phone to dial an outgoing call: remote user will see the telephone number - 5972726 because CLIP is not checked.

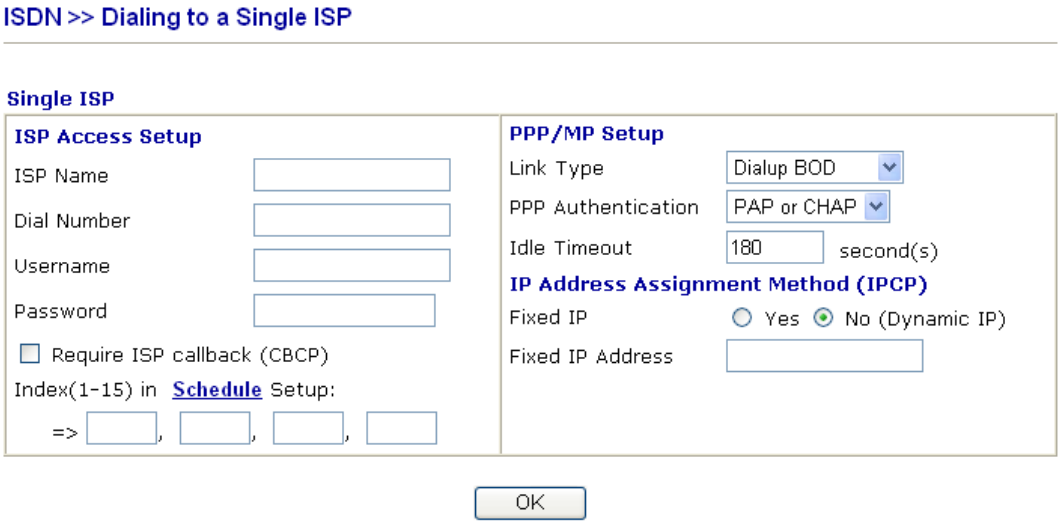
If you use ISDN1-S0 with **MSN 32** to dial an outgoing call: remote user will see “Withheld Number” from the telephone display panel because Phone CLIR is checked.

If you use **ISDN1-S0 with MSN 5972729** to dial an outgoing call: remote user will see the number 5972729 because Phone CLIP is checked.

If you use **ISDN1-S0 without MSN Setup** to dial an outgoing call: remote user will see the number 5972720 because Phone CLIP is checked.

3.12.3 Dial to Single/Dual ISPs

Select **Dialing to a Single ISP** if you access the Internet via a single ISP.



ISP Access Setup

ISP Name - Enter your ISP name such as Seednet, Hinet and so on.
Dial Number -Enter the ISDN access number provided by your ISP.
Username - Enter the username provided by your ISP.
Password - Enter the password provided by your ISP.
Require ISP Callback (CBCP) -If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation.
Scheduler (1-15) - Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules. Refer to section **3.8.2 Schedule** for detailed configuration.

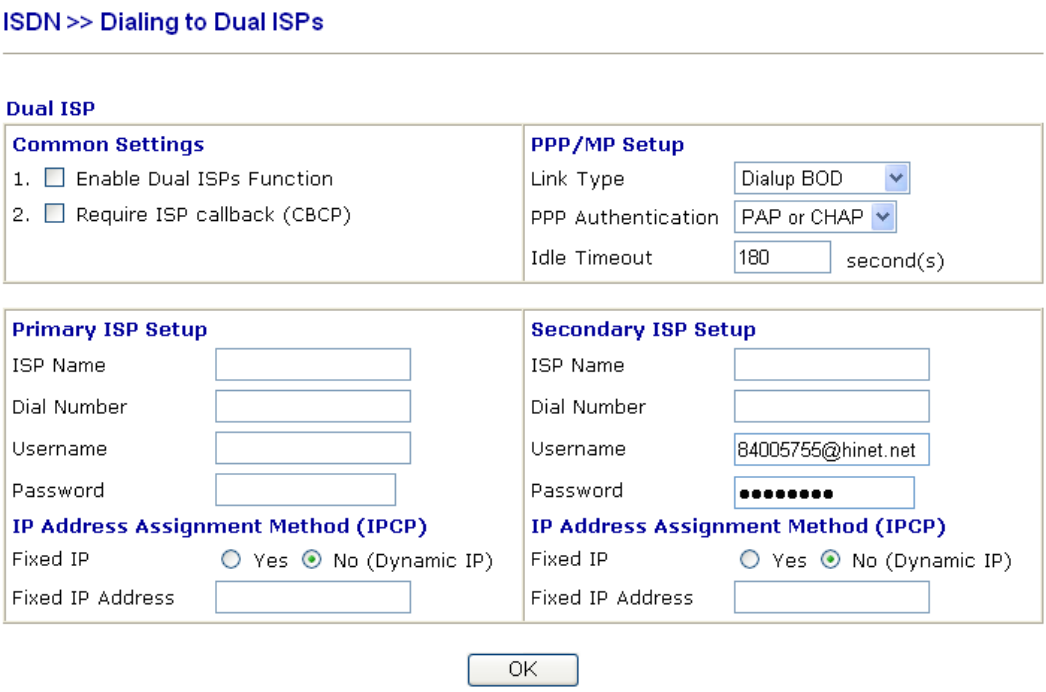
PPP/MP Setup

Link Type – There are three link types provided here for different purpose. **Link Disable** disables the ISDN dial-out function. **Dialup 64Kbps** allows you to use one ISDN B channel for Internet access. **Dialup 128Kbps** allows you to use both ISDN B channels for Internet access. **Dialup BOD** (for detailed information of configuration, please refer to section **3.12.4**) stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the section of **Call Control**.
PPP Authentication - PAP only allows you to configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP. **PAP or CHAP** is to configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.
Idle Timeout - Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.

IP Address Assignment Method (IPCP)

In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes** and enter the IP address in the field of **Fixed IP Address**.

Select **Dialing to Dual ISPs** if you have more than one ISP. You will be able to dial to both ISPs at the same time. This is mainly for those ISPs that do not support Multiple-Link PPP (ML-PPP). In such cases, dialing to two ISPs can increase the bandwidth utilization of the ISDN channels to 128kbps data speed.



Common Settings

Enable Dual ISPs Function - Check to enable the Dual ISPs function. **Require ISP Callback (CBCP) -**If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation.

PPP/MP Setup

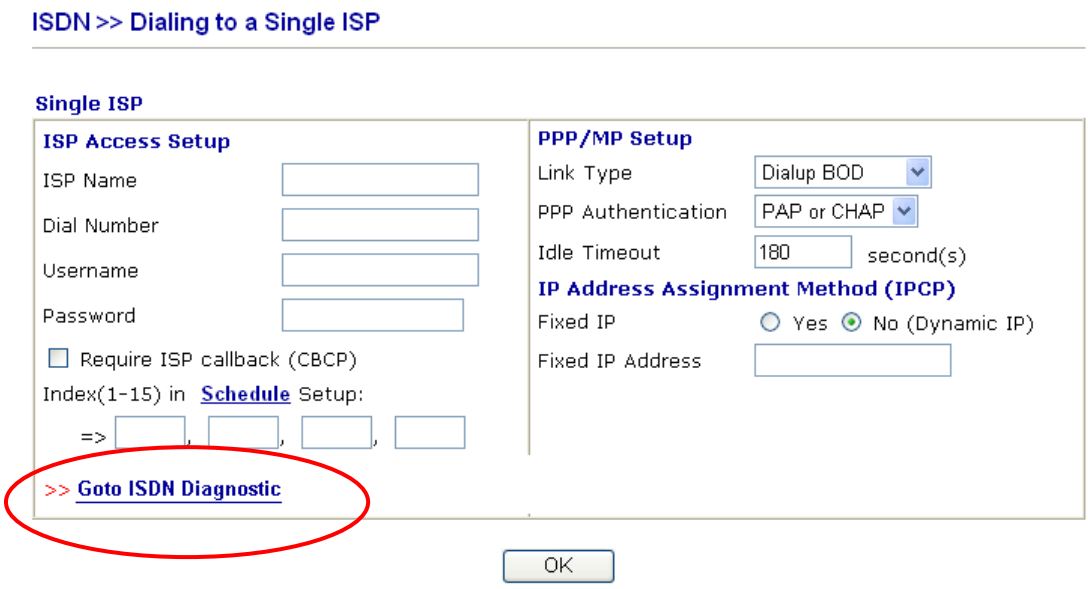
Link Type – There are three link types provided here for different purpose. **Link Disable** disables the ISDN dial-out function. **Dialup 128Kbps** allows you to use both ISDN B channels for Internet access. **Dialup BOD** (for detailed information of configuration, please refer to section **3.12.4**) stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup.

PPP Authentication - PAP only allows you to configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP. **PAP or CHAP** can configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.

Idle Timeout - Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.

Primary ISP Setup	**ISP Name -** Enter your ISP name. **Dial Number -**Enter the ISDN access number provided by your ISP. **Username -** Enter the username provided by your ISP. **Password -** Enter the password provided by your ISP.
IP Address Assignment Method (IPCP) for primary ISP setup	In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes** and enter the IP address in the field of **Fixed IP Address**.
Secondary ISP Setup)	**ISP Name -** Enter the secondary ISP name. **Dial Number -**Enter the ISDN access number provided by the ISP. **Username -** Enter the username provided by your ISP. **Password -** Enter the password provided by your ISP.
IP Address Assignment Method (IPCP) for secondary ISP setup	In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes** and enter the IP address in the field of **Fixed IP Address**.

After entering the necessary settings and clicking **OK**, you will see **Goto ISDN Diagnostic** link appears on the bottom of the webpage.



To have an ISDN connection, please click **Goto ISDN Diagnostic**. The following page will be displayed on your screen.

Diagnostics >> WAN Connection

ISDN/PPPoE/PPPoA Diagnostics | Refresh |

ISDN Link Status	UP	
Internet Access	>> Dial ISDN	
B Channel	B1	B2
Activity	Idle	Idle
Drop Connection	>> Drop B1	>> Drop B2
Broadband Access Mode/Status	---	
Internet Access	>> Dial PPPoE/PPPoA	
WAN IP Address	---	
Internet Access	>> Dial PPPoE/PPPoA	
Drop Connection	>> Drop PPPoE/PPPoA	

Click **Dial ISDN**. Wait for a moment after clicking the dial link. Then, a successful ISDN connection will be shown as the following.

Yes Ethernet Static IP 00:00:00

IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
172.17.3.43	172.17.3.2	0	0	0	0

ADSL Information (ADSL Firmware Version: 2121501_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	0	0	0	0

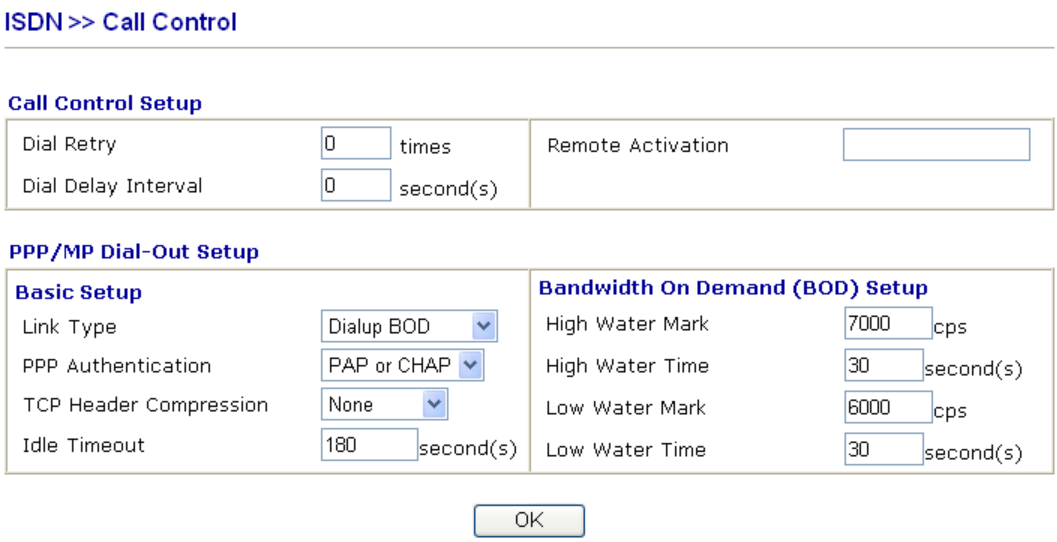
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	-----	READY	0	0	0	0

ISDN Status >> Dial ISDN >> Drop B1 >> Drop B2

Channel	Active Connection	TX Pkts	TX Rate (Bps)	RX Pkts	RX Rate (Bps)	Up Time	AOC
ISDN1-B1	Idle [---]	0	0	0	0	0:0:0	0
ISDN1-B2	Idle [---]	0	0	0	0	0:0:0	0
ISDN1-D	UP						
ISDN2-B1	2930 [192.168.3.10]	19	9	10	3	0:0:36	0
ISDN2-B2	Idle [---]	0	0	0	0	0:0:0	0
ISDN2-D	UP						

3.12.4 Call Control

Some applications require that the router (only for the ISDN models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature by allowing user to make a phone call to the router and then ask it to dial up to the ISP. Accordingly, a teleworker can access the remote network to retrieve resources. Of course, a fixed IP address is required for WAN connection and some internal network resource has to be exposed for remote users, such as FTP, WWW.



Call Control Setup

Dial Retry - It specifies the dial retry counts per triggered packet. A triggered packet is the packet whose destination is outside the local network. The default setting is no dial retry. If set to 5, for each triggered packet, the router will dial 5 times until it is connected to the ISP or remote access router.
Dial Delay Interval - It specifies the interval between dialup retries. By default, the interval is 0 second.
Remote Activation – It can help users who would like to access the server which is off the Internet in the head office. To remotely make the server to be available on the Internet, i.e. make the router in the head office activating its Internet access either by dialing-up or starting broadband connection, users can make a regular phone call (the number is set in the Remote Activation field) to the router as signaling it for activation. The phone call will be soon disconnected once the router is on line.

> Note that **Dialing to a Single ISP** should be pre-configured properly.

Basic Setup

Link Type - Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel, two B channels or BOD (Bandwidth on Demand). Four options are available: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD.

PPP Authentication - It specifies the PPP authentication

method for PPP/MP connections. Normally you can set it to PAP/CHAP for better compatibility.
TCP Header Compression - VJ Compression: It is used for TCP/IP protocol header compression. Normally it is set to Yes to improve bandwidth utilization.
Idle Timeout - Because our IDSN link type is **Dial On Demand**, the connection will be initiated only when needed.

Bandwidth-On-Demand (BOD) Setup

Bandwidth-On-Demand is for Multiple-Link PPP \(ML-PPP or MP). The parameters are only applied when you set the **Link Type** to **Dialup BOD**. The ISDN usually use one B channel to access the Internet or remote network when you choose the Dialup BOD link type. The router will use the parameters here to decide on when you activate/drop the additional B channel. Note that **cps** (characters-per-second) measures the total link utilization.
High Water Mark and High Water Time - These parameters specify the situation in which the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is being used over the High Water Time, the additional channel will be activated. Thus, the total link speed will be 128kbps (two B channels).

Low Water Mark and Low Water Time - These parameters specify the situation in which the second channel will be dropped. In terms of the two B channels, if their utilization is under the Low Water Mark and these two channels are being used over the High Water Time, the additional channel will be dropped. As a result, the total link speed will be 64kbps (one B channel).

3.13 Wireless LAN

This function is used for “n” models only.

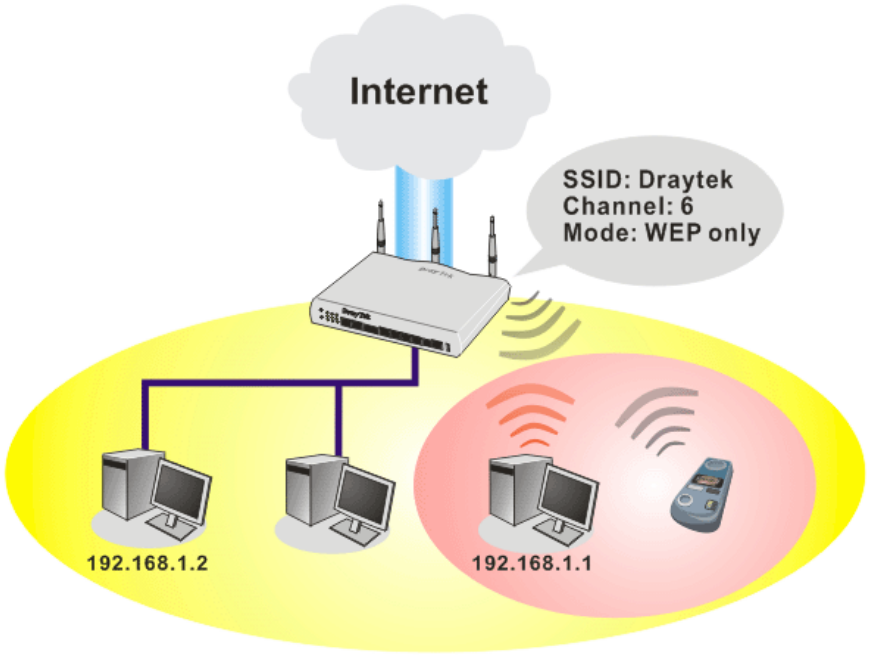
3.13.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor “n” model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

> **Note**: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Security Overview

Real-time Hardware Encryption: Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

Complete Security Standard Selection: To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

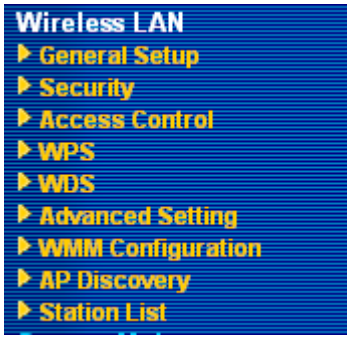
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

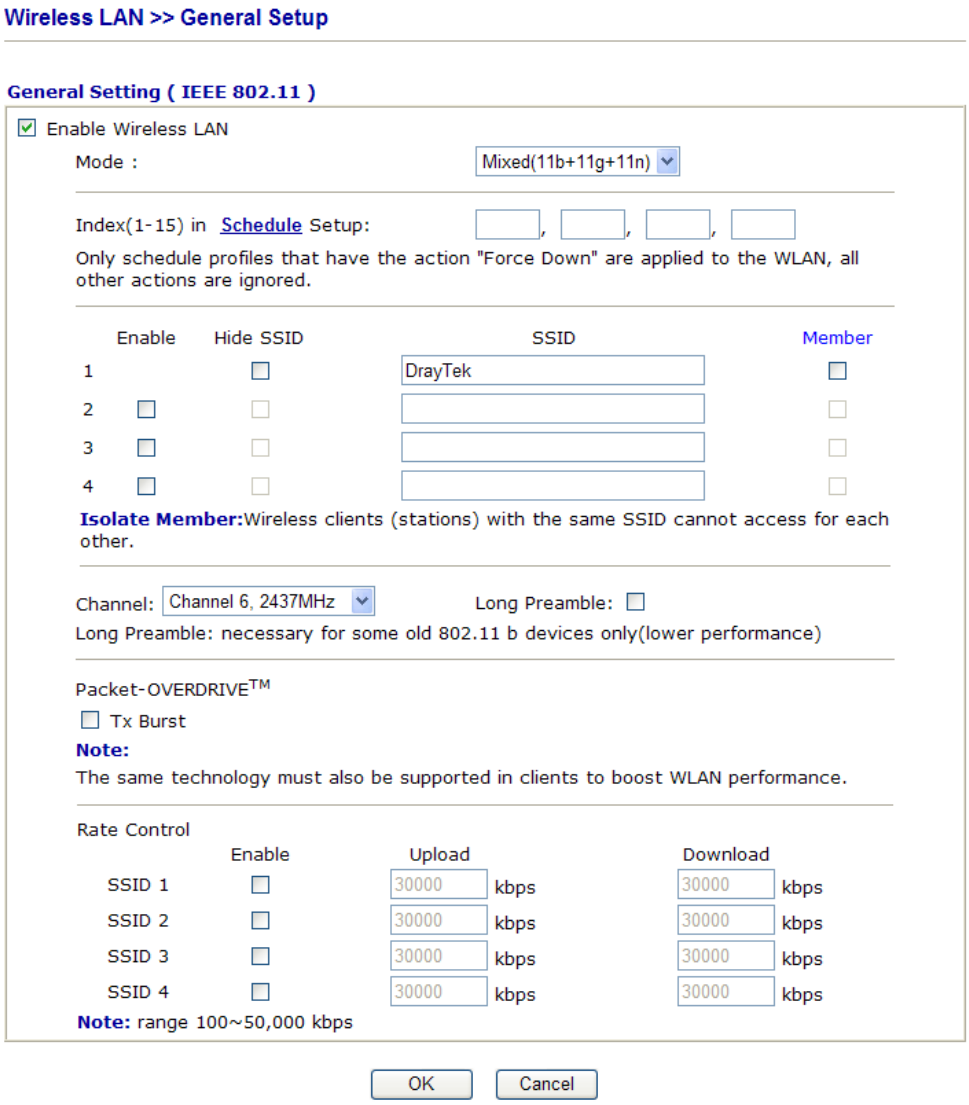
Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.

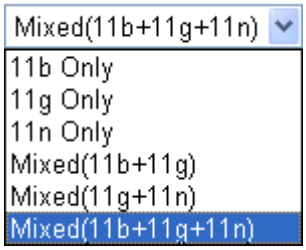


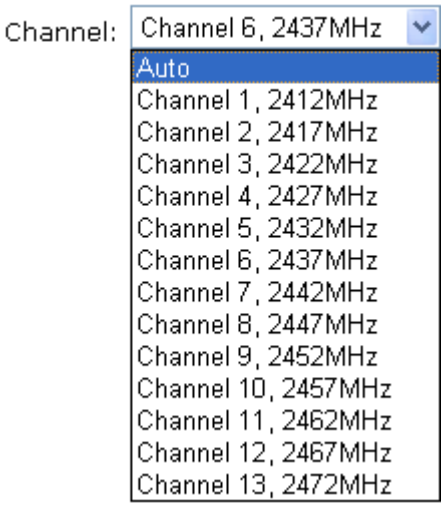
3.13.2 General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.



Enable Wireless LAN Check the box to enable wireless function.

Mode	At present, the router can connect to 11b Only, 11g Only, 11n Only, Mixed(11b+11g), Mixed(11g+11n) and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode. 
Index(1-15)	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications** >> **Schedule** setup. The default setting of this filed is blank and the function will always work.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "default". We suggest you to change it.
Isolate	**Member** –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.



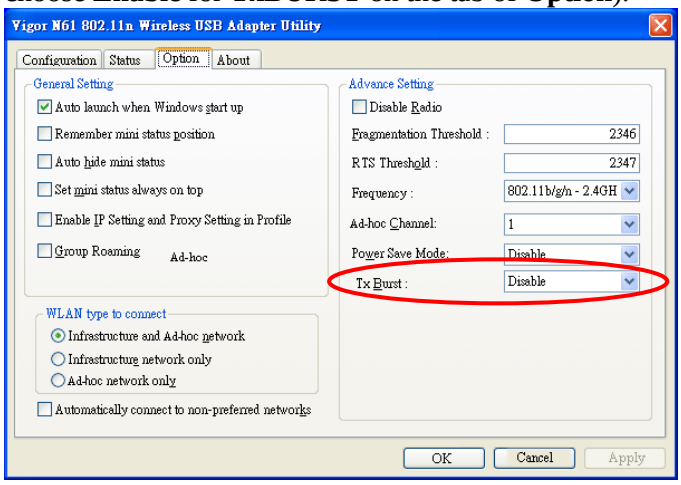
Long Preamble

This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

Packet-OVERDRIVE

This feature can enhance the performance in data transmission about 40% for 11g (5% for 11n) by checking **Tx Burst**. It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).



Rate Control

It controls the data transmission rate through wireless connection.

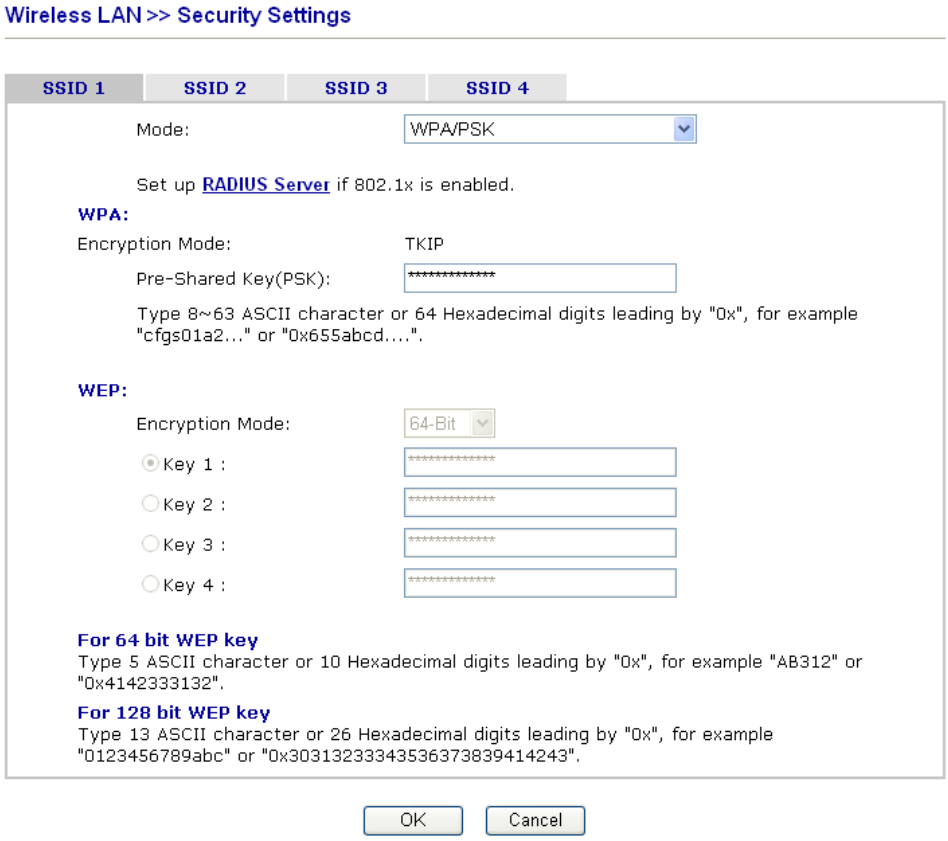
Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.

Download – Type the transmitting rate for data download. Default value is 30,000 kbps.

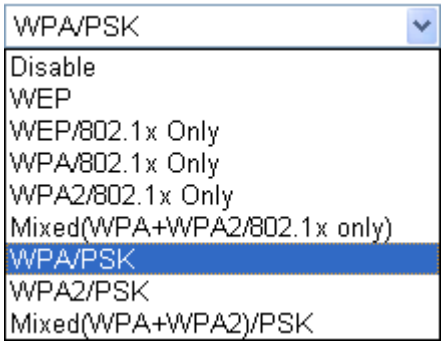
3.13.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.


Wireless LAN >> Security Settings
SSID 1
SSID 2
SSID 3
SSID 4
Mode:
WPA/PSK
Set up RADIUS Server if 802.1x is enabled.
WPA:
Encryption Mode:
TKIP
Pre-Shared Key(PSK):
Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".
WEP:
Encryption Mode:
64-Bit
Key 1 :
Key 2 :
Key 3 :
Key 4 :
For 64 bit WEP key
Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132".
For 128 bit WEP key
Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".
OK
Cancel

Mode There are several modes provided for you to choose.



Disable - Turn off the encryption mechanism.
WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.
WEP/802.1x Only - Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
WPA/802.1x Only- Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

WPA2/802.1x Only- Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
Mixed (WPA+WPA2/802.1x only) - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.
WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.
WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.
Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.

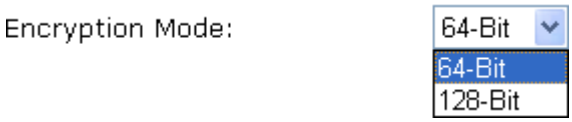
> **Note:** You should also set RADIUS Server simultaneously if WEP/802.1x Only, WPA/802.1x Only, WPA2/802.1x Only or Mixed (WPA+WPA2/802.1x only) is selected.

WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Type - Select from Mixed (WPA+WPA2) or WPA2 only.
Pre-Shared Key (PSK) - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

WEP

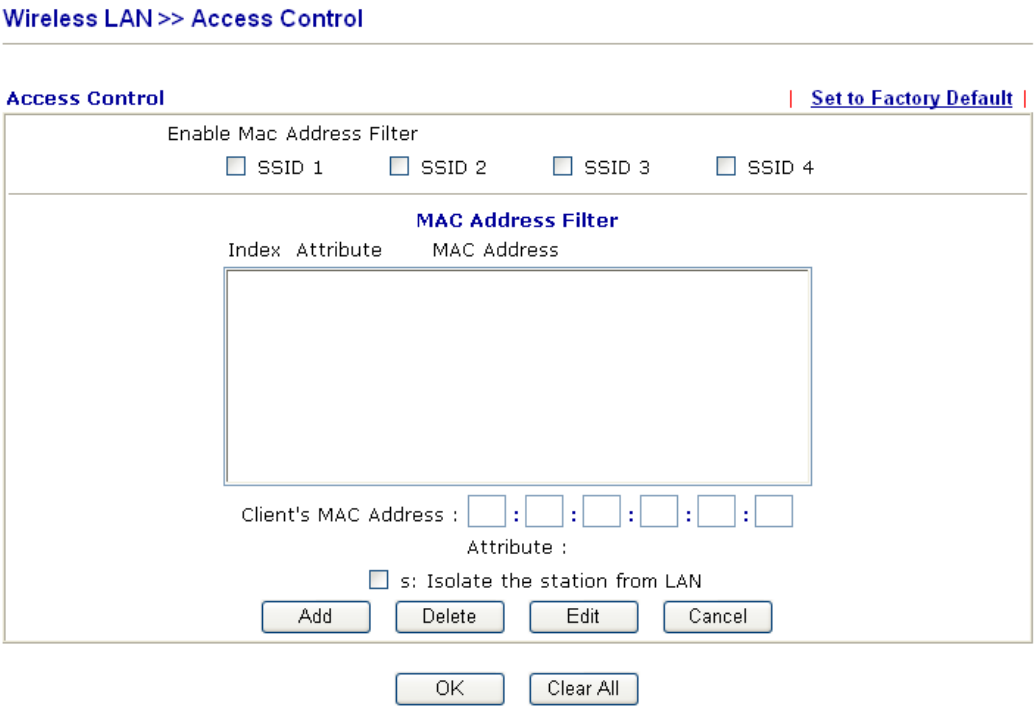
64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
128-Bit - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D).



All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

3.13.4 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights.

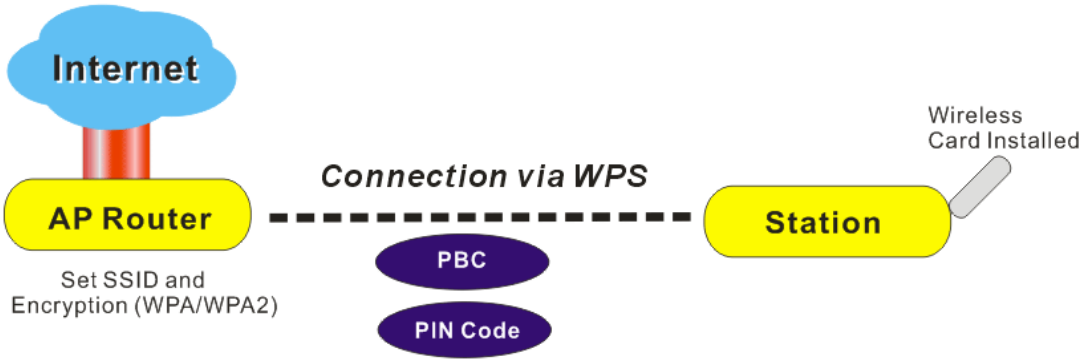


Enable Max Access Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Attribute	**s: Isolate the station from LAN -** select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

Clear All	Clean all entries in the MAC address list.

3.13.5 WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

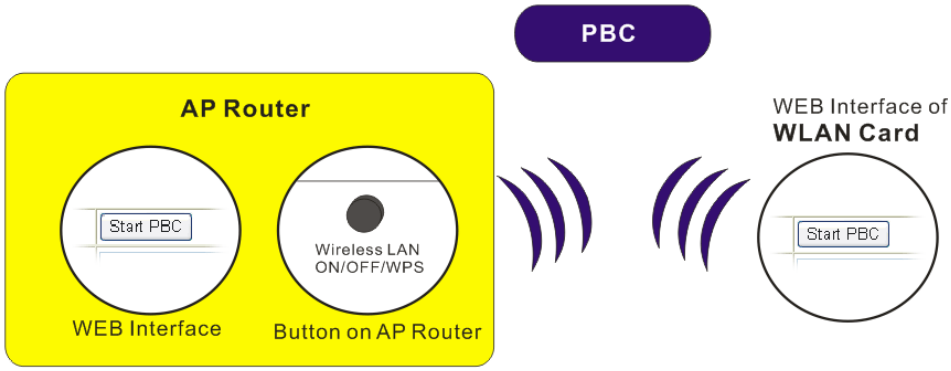


Note: Such function is available for the wireless station with WPS supported.

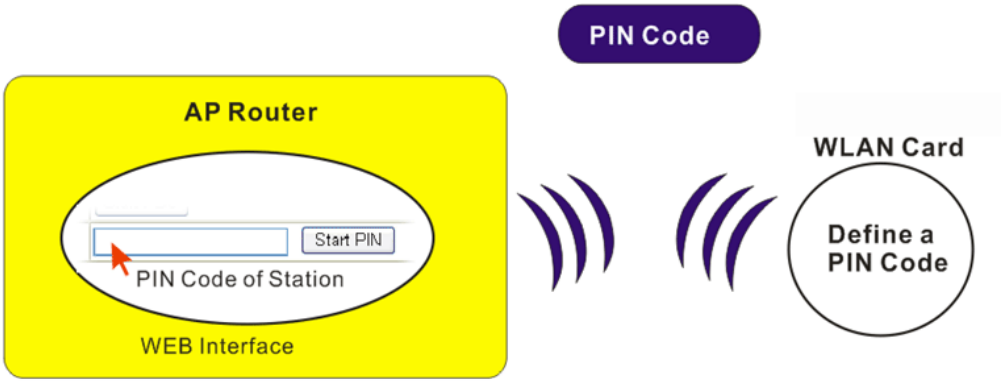
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press the **WPS** button on AP and selects that AP on the utility of wireless station. Then WPS will connect for client and router automatically.

There are two methods to do network connection through WPS between AP and Stations: pressing the ***Start PBC*** button or using ***PIN Code***.

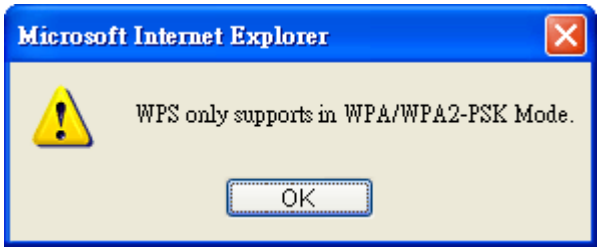
- On the side of Vigor 2820 series which served as an AP, press **Wireless LAN ON/OFF/WPS** button for 2 seconds to wait for client device making network connection through WPS or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



- If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the vigor router.



For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

Below shows **Wireless LAN>>WPS** web page.

Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.

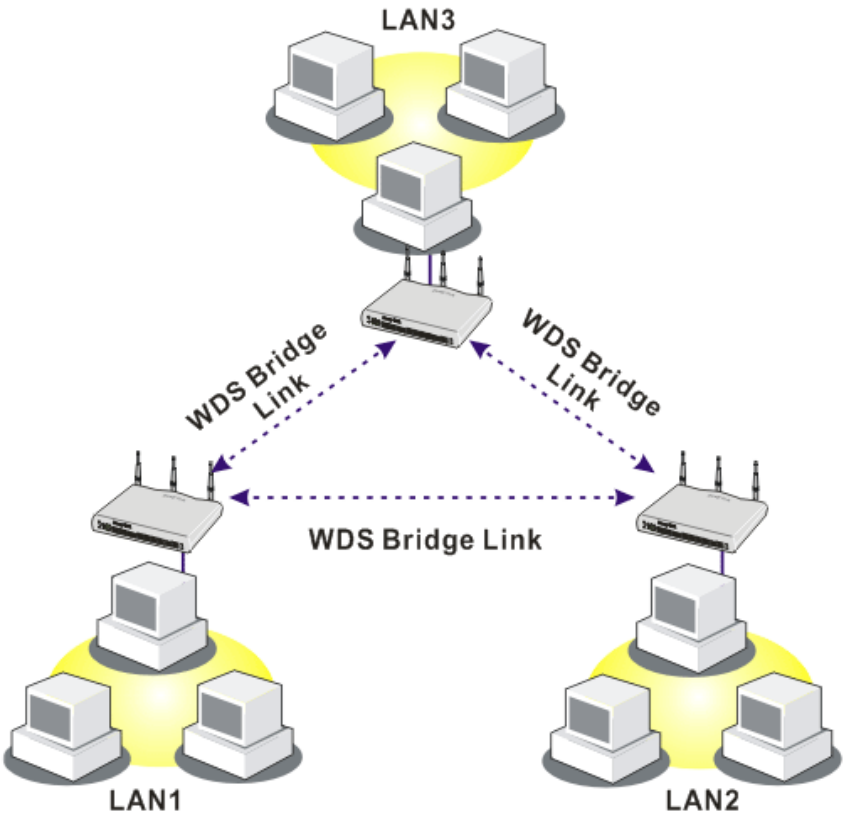
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

3.13.6 WDS

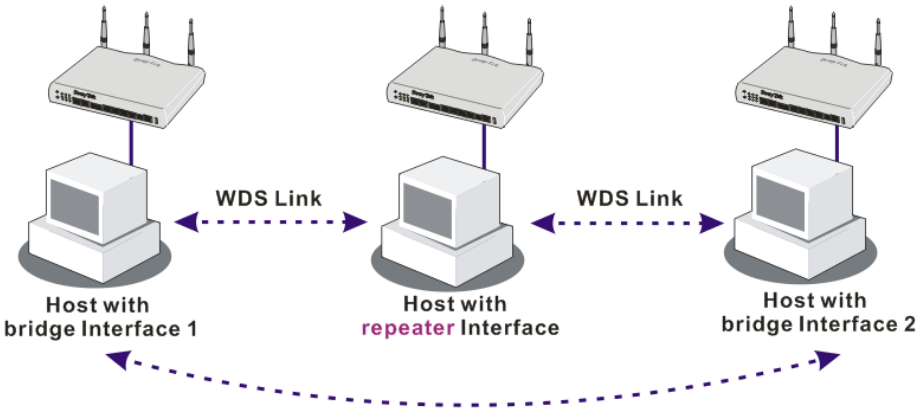
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

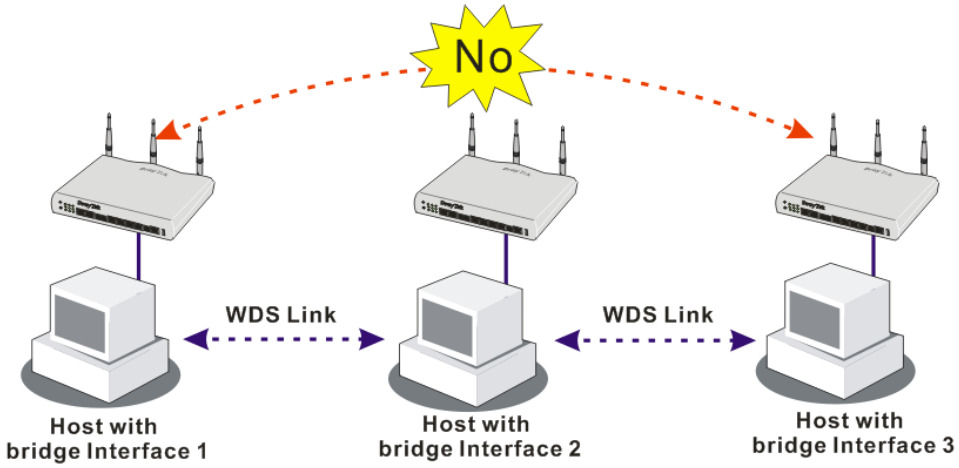


The application for the WDS-Repeater mode is depicted as below:

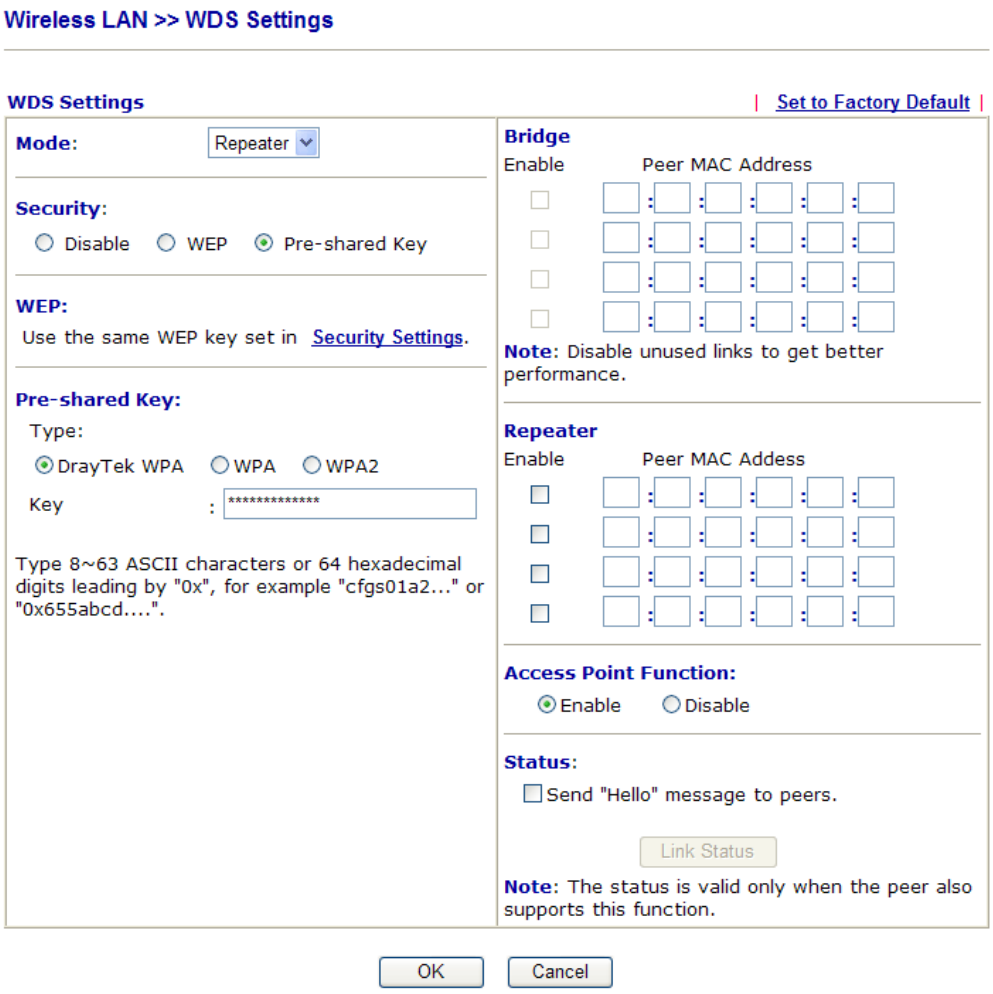


The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

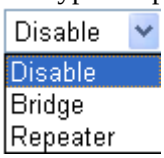
In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.



Mode Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the first type of application. **Repeater** mode is for the second one.



Security There are three types for security, **Disable**, **WEP** and **Pre-shared key**. The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.

WEP Check this box to use the same key set in **Security Settings** page. If you did not set any key in **Security Settings** page, this check box will be dimmed.

Pre-shared Key **Type –** There are three types for you to choose. **DrayTek WPA** can be used for all DrayTek wireless routers like Vigor2700, Vigor2800, Vigor2820, and etc., except for other brand's wireless routers. **WPA** and **WPA2** are used for WDS devices (e.g., AP700). For example, if you have a wireless AP and a Vigor2820n wireless router, you can set the encryption mode as WPA or WPA2 to establish your WDS system between AP and the router.

Key - Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.

Bridge — If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.

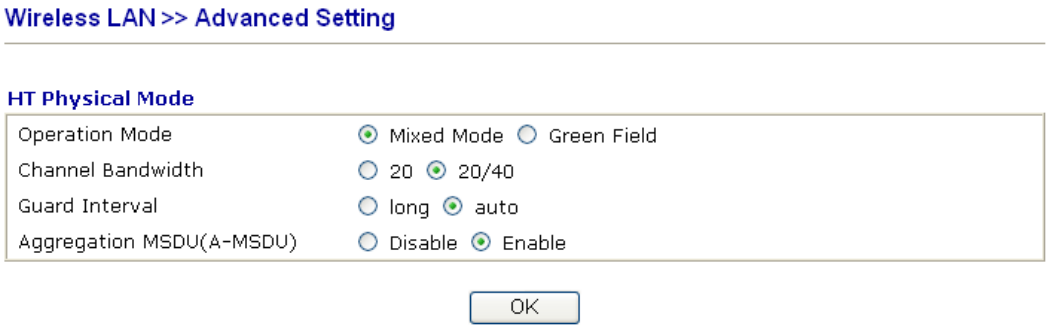
Repeater — If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing.

Access Point Function — Click **Enable** to make this router serving as an access point; click **Disable** to cancel this function.

Status — It allows user to send “hello” message to peers. Yet, it is valid only when the peer also supports this function.

3.13.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.



Operation Mode — **Mixed Mode** – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.
Green Field – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.

Channel Bandwidth — **20-** the router will use 20Mhz for data transmission and receiving between the AP and the stations.
20/40 – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.

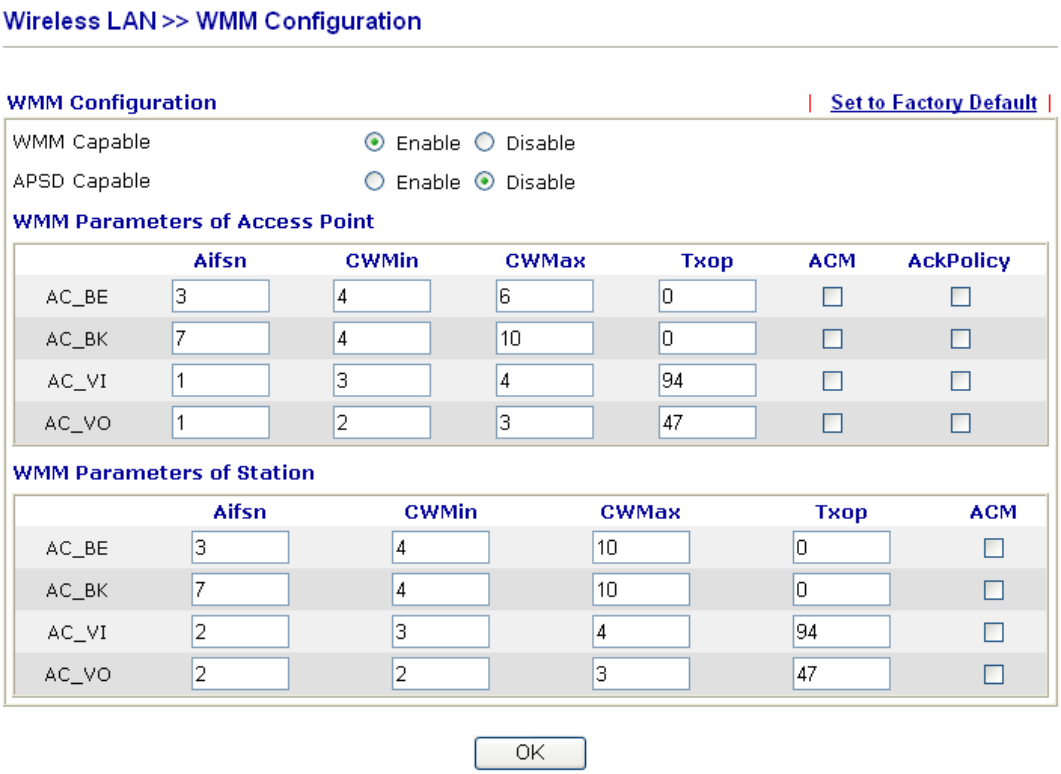
Guard Interval — It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose **auto** as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.

Aggregation MSDU Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is **Enable.**

3.13.8 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE , AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. Such function is designed for mobile and cordless phones that support VoIP mostly.



WMM Capable To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.

APSD Capable The default setting is **Disable**.

Aifsn It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories. As to the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.

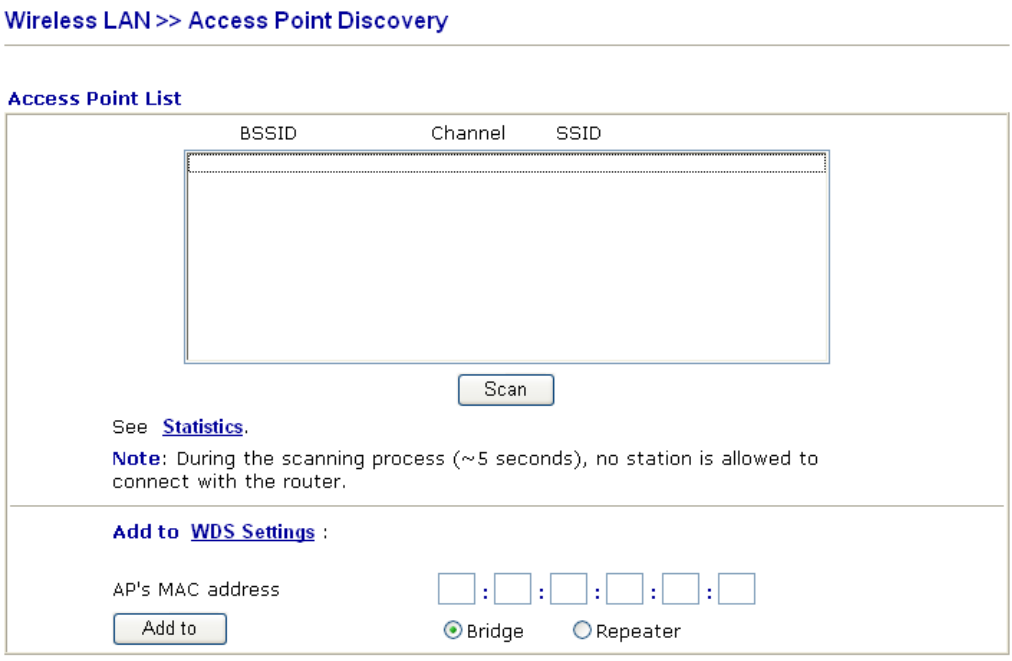
CWMin/CWMax **CWMin** means contention Window-Min and **CWMax** means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller;

	however, the difference between AC_BE and AC_BK categories must be greater.
Txop	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission Control Mandatory. It can restrict stations from using specific category class if it is checked. **Note:** Vigor2820 provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	**"**Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets. "Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.

3.13.9 AP Discovery

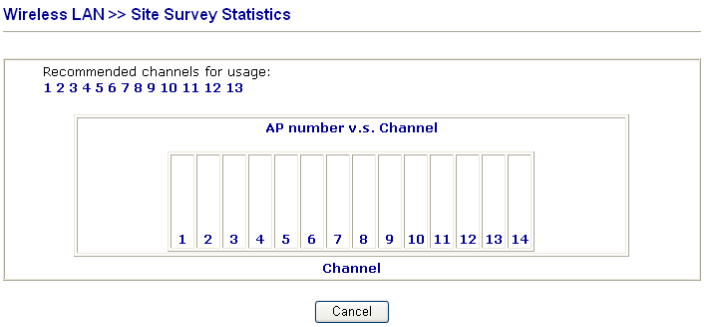
Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.



Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.

Statistics It displays the statistics for the channels used by APs.


Wireless LAN >> Site Survey Statistics
Recommended channels for usage:
1 2 3 4 5 6 7 8 9 10 11 12 13
AP number v.s. Channel
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Channel
Cancel

Add to If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page or choose the AP MAC address from the Scan result field, and click **Bridge** or **Repeater**. Next, click **Add to**. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

3.13.10 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

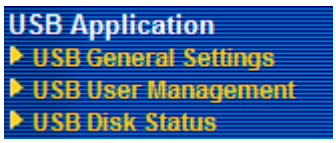
Wireless LAN >> Station List
Station List
Status
MAC Address
Associated with
Refresh
Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass 802.1X or WPA/PSK authentication.
Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.
Add to Access Control :
Client's MAC address
Add

Refresh Click this button to refresh the status of station list.

Add Click this button to add current selected MAC address into **Access Control**.

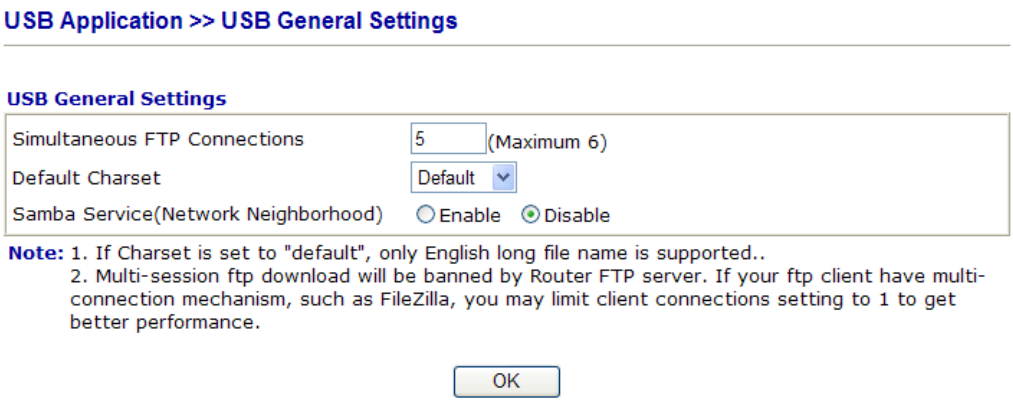
3.14 USB Application

USB diskette can be regarded as a server. By way of Vigor router, clients on LAN can access, write and read data stored in USB diskette. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the FTP client software. Thus, the client can use the FTP site (USB diskette)or share the Samba service through Vigor router.



3.14.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable Samba service. At present, the Vigor router can support USB diskette with versions of FAT16 and FAT32 only. Therefore, before connecting the USB diskette into the Vigor router, please make sure the memory format for the USB diskette is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).


USB Application >> USB General Settings
USB General Settings
Simultaneous FTP Connections
5
(Maximum 6)
Default Charset
Default
Samba Service(Network Neighborhood)
Enable
Disable
Note: 1. If Charset is set to "default", only English long file name is supported..
2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multi-connection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.
OK

Simultaneous FTP Connection This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage diskette at one time.

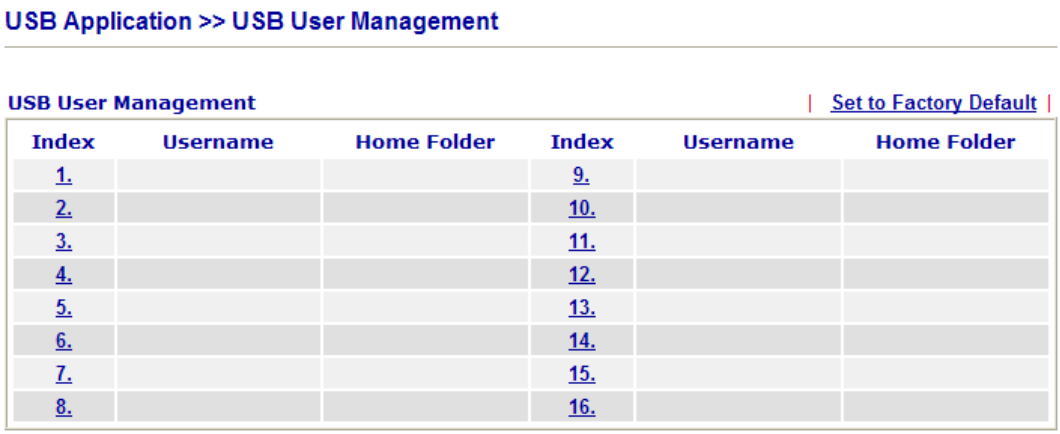
Default Charset At present, Vigor router supports three types of character sets: default, GB2312 and BIG5.

Default Charset is for English based file name. For Simplified Chinese file/directory names, please choose GB2312; for Traditional Chinese file/directory names, choose BIG5.

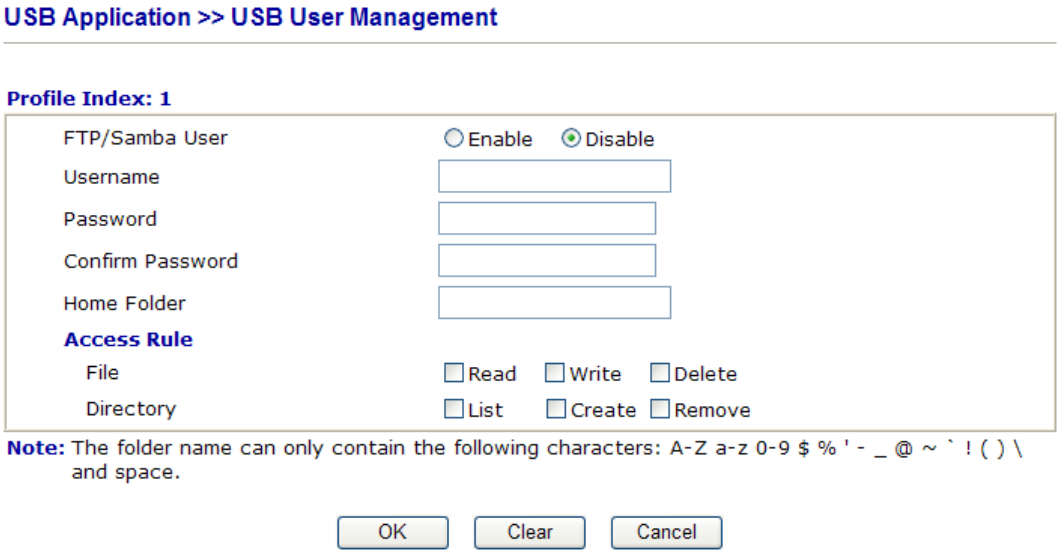
Samba Service Click **Enable** to invoke samba service via the router.

3.14.2 FTP User Management

This page allows you to set profiles for FTP users. Any user who wants to access into the USB diskette must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB diskette first. Otherwise, an error message will appear to warn you.



Click index number to access into configuration page.



FTP/Samba User

Enable – Click this button to activate this profile (account) for FTP service or Samba User service. Later, the user can use the username specified in this page to login into FTP server.

Disable – Click this button to disable such profile.

Username

Type the username for FTP users for accessing into FTP server (USB diskette). Be aware that users cannot access into USB diskette in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage diskette.

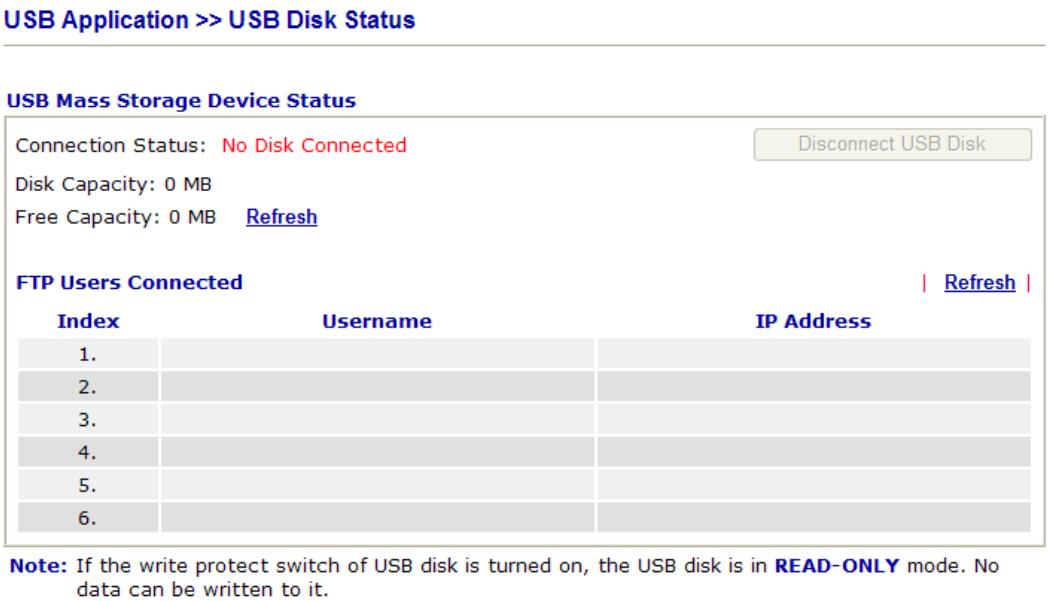
Note: "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.

Password	Type the password for FTP users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage diskette.
Confirm Password	Type the password again to make confirmation.
Home Folder	It determines the range for the client to access into. The user can enter a directory name in this field. Then, after clicking OK, the router will create the specific/new folder in the USB diskette. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB diskette. **Note:** When write protect status for the USB diskette is **ON**, you cannot type any new folder name in this field. Only "/" can be used in such case.
Access Rule	It determines the authority for such profile. Any user, who uses such profile for accessing into USB diskette, must follow the rule specified here. **File** – Check the items (Read, Write and Delete) for such profile. **Directory** –Check the items (List, Create and Remove) for such profile.

Before you click **OK**, you have to insert a USB diskette into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

3.14.3 Disk Status

This page is to monitor the status for the FTP users who accessing into FTP server (USB diskette) via the Vigor router. If you want to remove the diskette from USB port in router, please check the box of Safely Remove Disk first. And then, remove the USB diskette later.



Connection Status	If there is no USB diskette connected to Vigor router, "**No Disk Connected**" will be shown here.
Disk Capacity	It displays the total capacity of the USB diskette.

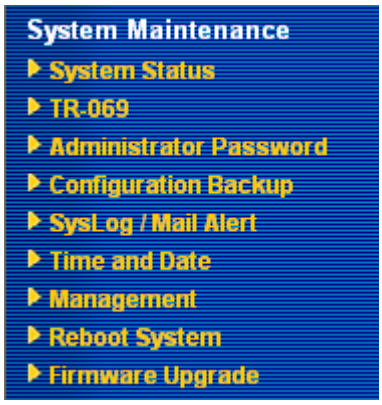
Free Capacity	It displays the free space of the USB diskette. Click **Refresh** at any time to get new status for free capacity.
Username	It displays the username that user uses to login to the FTP server.
IP Address	It displays the IP address of the user's host which connecting to the FTP server.

When you insert USB diskette into the Vigor router, the system will start to find out such device within several seconds.?

3.15 System Maintenance

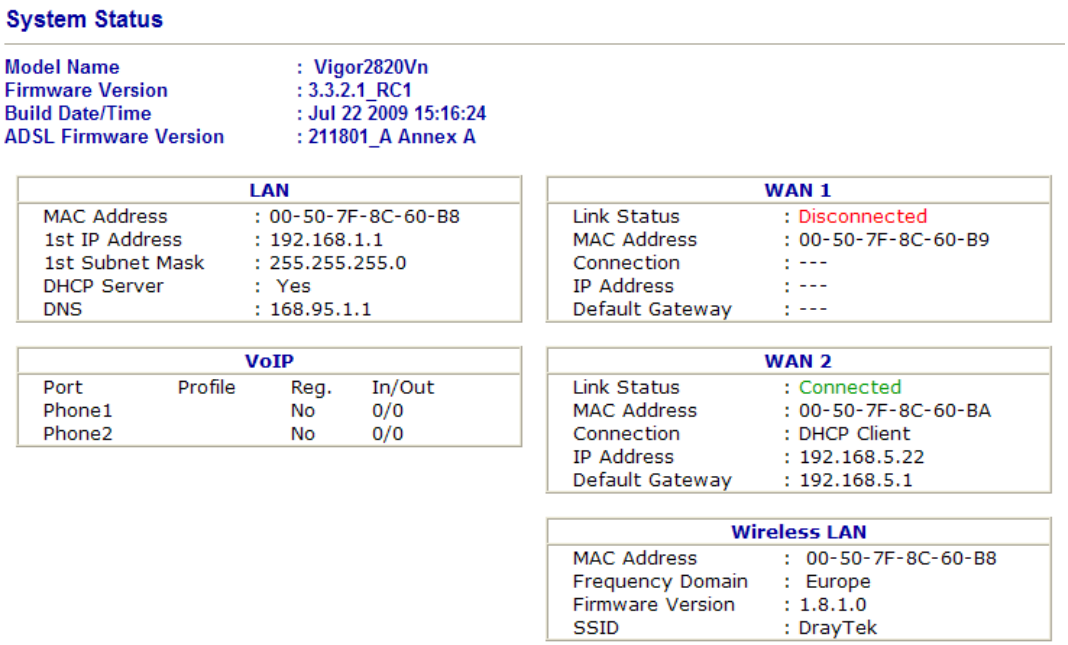
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



3.15.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

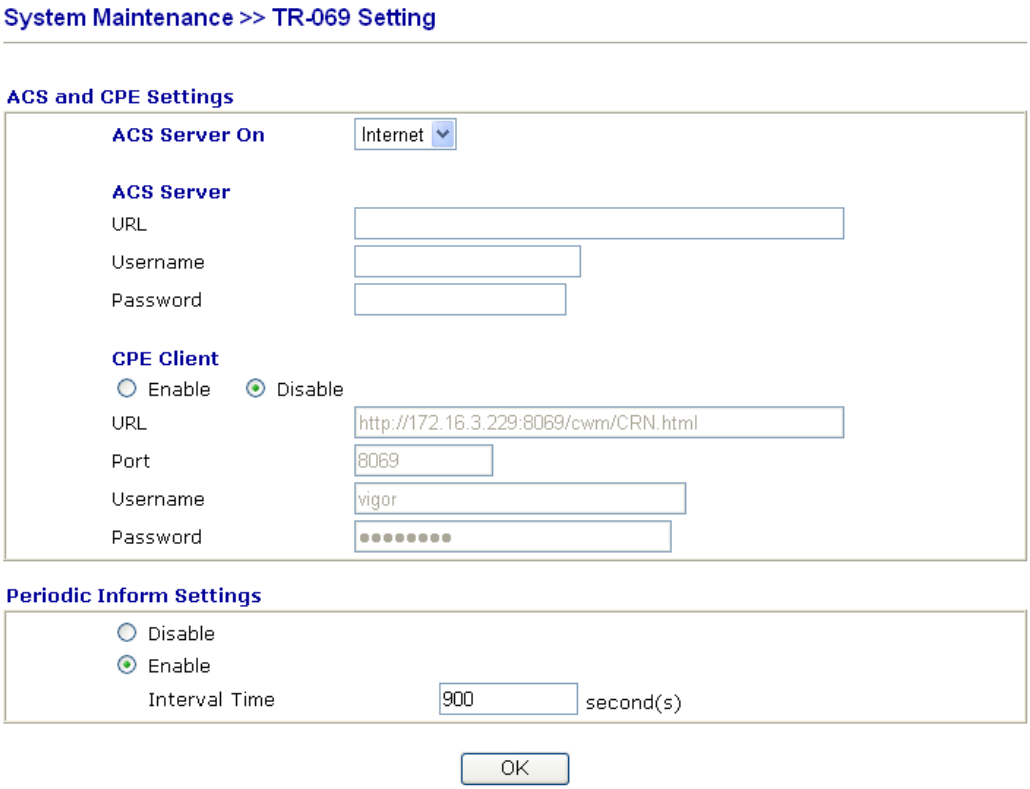


Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
ADSL Firmware Version	Display the ADSL firmware version.
LAN-------	
MAC Address	Display the MAC address of the LAN Interface.
1st IP Address	Display the IP address of the LAN interface.
1st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
WAN-------	
Link Status	Display current connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
Wireless LAN-------	
MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.

Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.
SSID	Display the SSID of the router.

3.15.2 TR-069

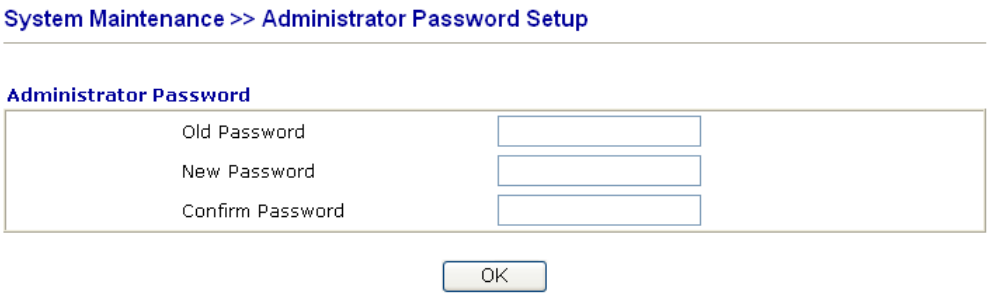
This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.



ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	**URL/Username/Password –** Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
CPE Client	It is not necessary for you to type them. Such information is useful for Auto Configuration Server. **Enable/Disable** – Sometimes, port conflict might be occurred. To solve such problem, you might want to change port number for CPE. Please click Enable and change the port number.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the router to send notification to CPE. Or click **Disable** to close the mechanism of notification.

3.15.3 Administrator Password

This page allows you to set new password.



Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this filed.
Confirm Password	Type in the new password again.

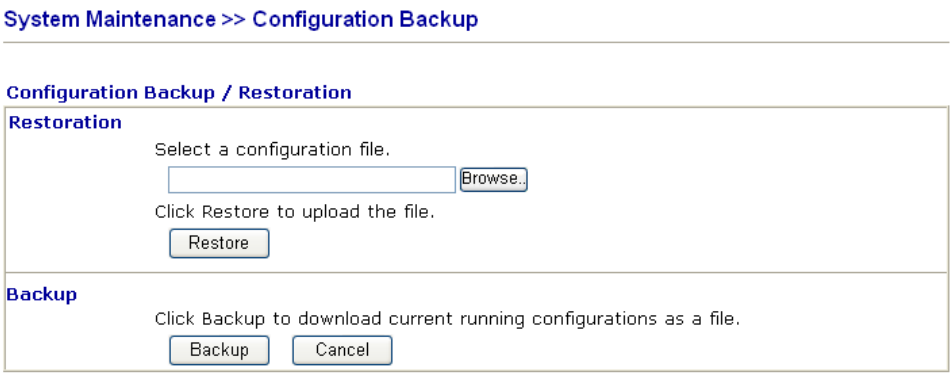
When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

3.15.4 Configuration Backup

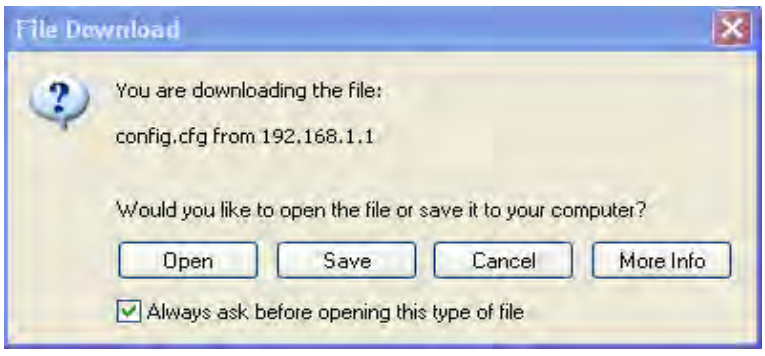
Backup the Configuration

Follow the steps below to backup your configuration.

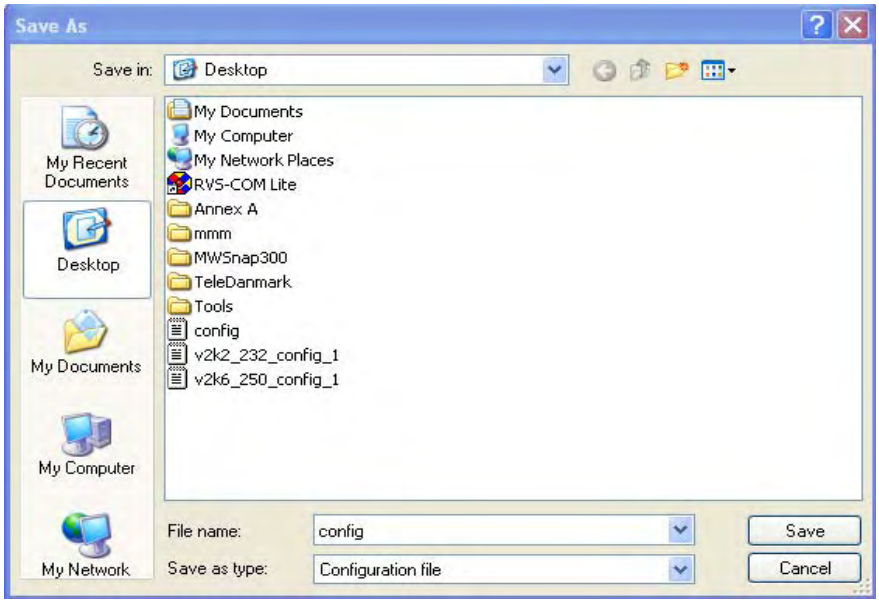
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.


File Download
You are downloading the file:
config.cfg from 192.168.1.1
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



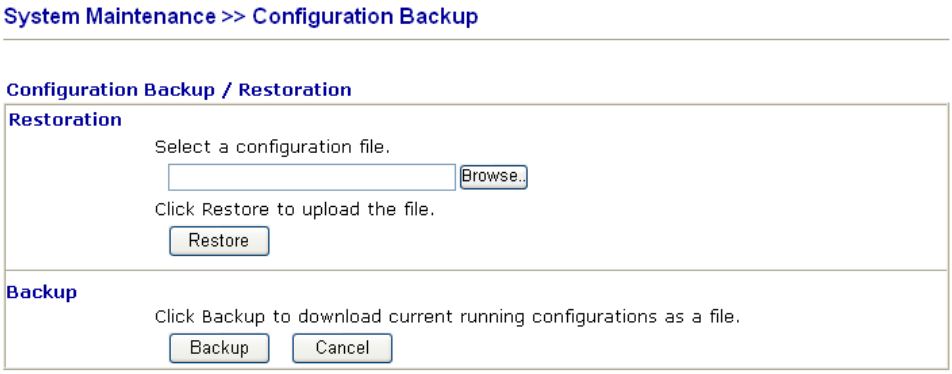
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

> **Note:** Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

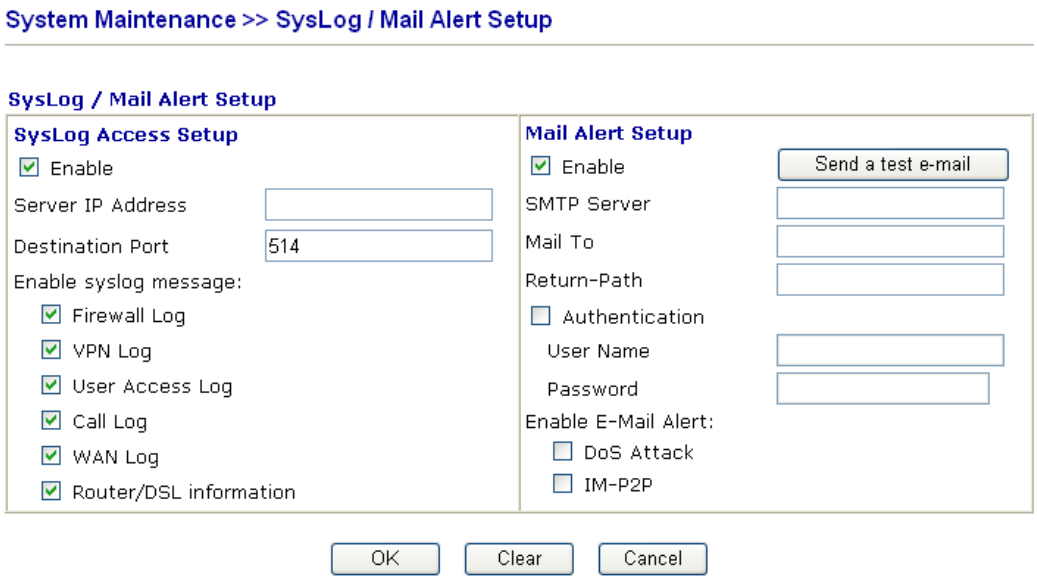
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



2. Click **Browse** button to choose the correct configuration file for uploading to the router.
3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

3.15.5 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

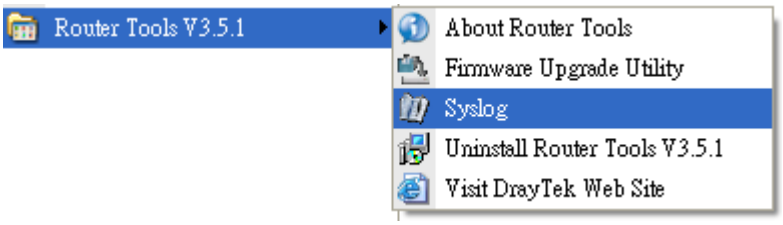


Enable (Syslog Access…)	Check "**Enable**" to activate function of syslog.
Syslog Server IP	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
Enable (Alert Setup…)	Check "**Enable**" to activate function of mail alert.
Send a test e-mail	Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign an e-mail address of another mailbox to accept all returned messages if fatal problems occur at the recipient mailbox. The e-mail address typed here also acts as the Sender address while Vigor sends out the alert e-mails.
Authentication	Check this box to activate this function while using e-mail application.
User Name	Type the user name for authentication.
Password	Type the password for authentication.
Enable E-mail Alert	Check the box to send alert message to the e-mail box while the modem detecting the item(s) you specify here.

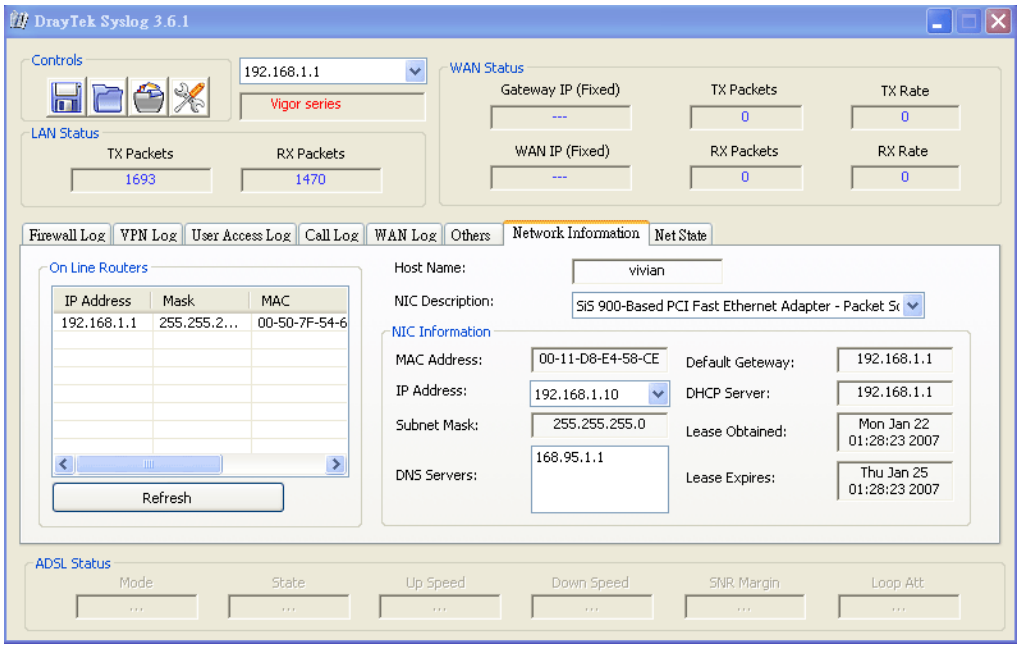
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.

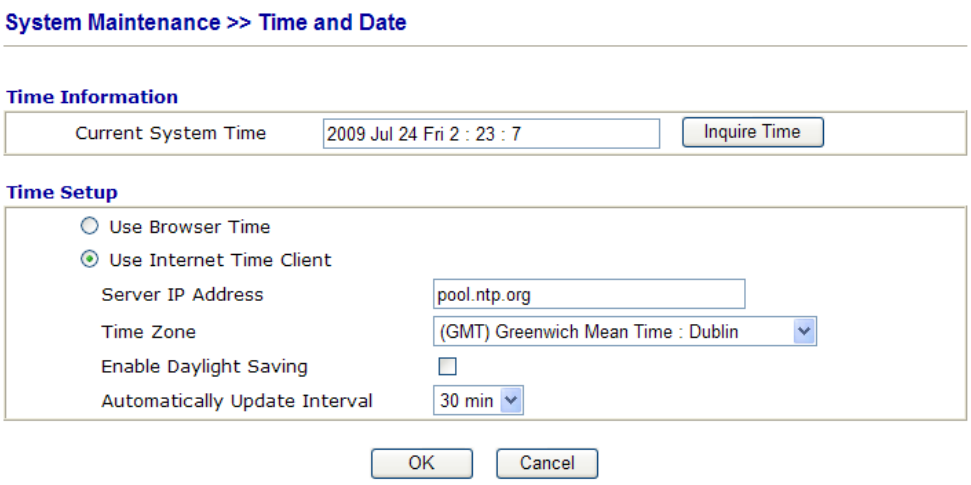


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



3.15.6 Time and Date

It allows you to specify where the time of the router should be inquired from.

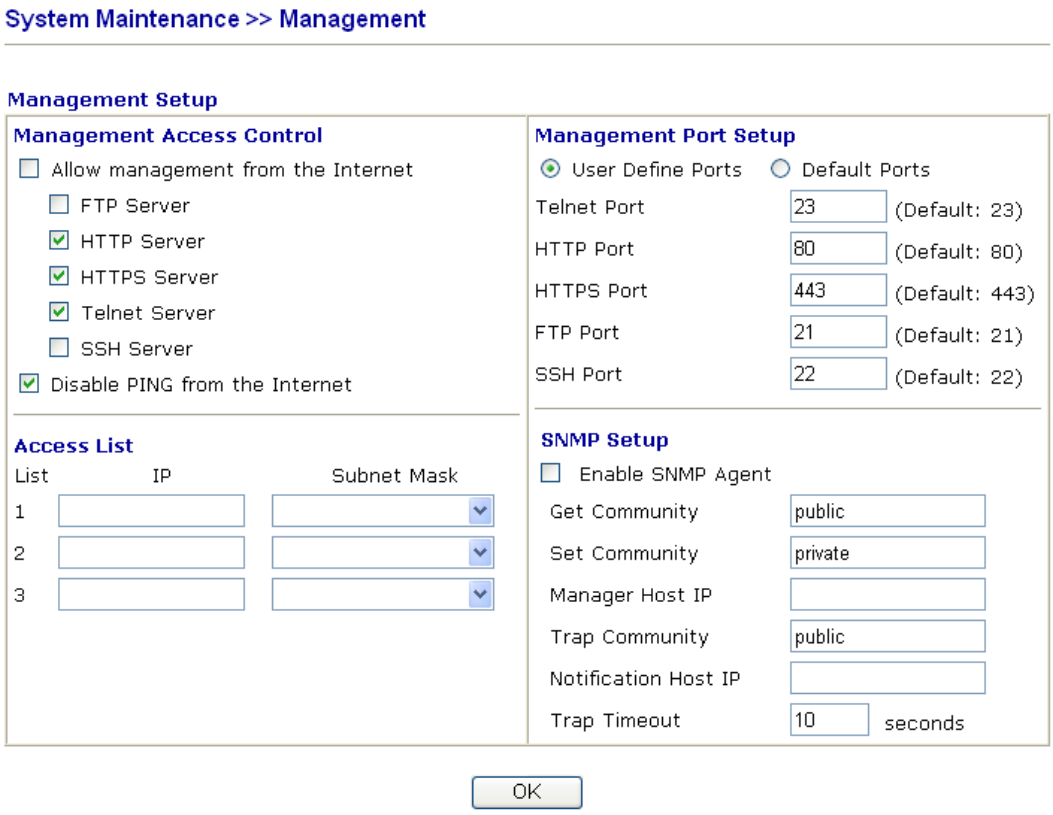


Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Server IP Address	Type the IP address of the time server.
Time Zone	Select the time zone where the router is located.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.15.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

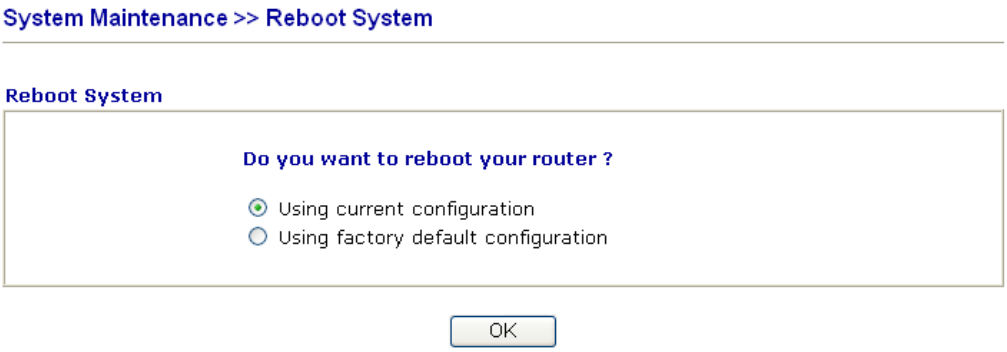


Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. **List IP** - Indicate an IP address allowed to login to the router. **Subnet Mask** - Represent a subnet mask allowed to login to the router.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is **public.**

Set Community	Set community by typing a proper name. The default setting is **private.**
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is **public.**
Notification Host IP	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

3.15.8 Reboot System

The Web Configurator may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.



If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 5 seconds to reboot the system.

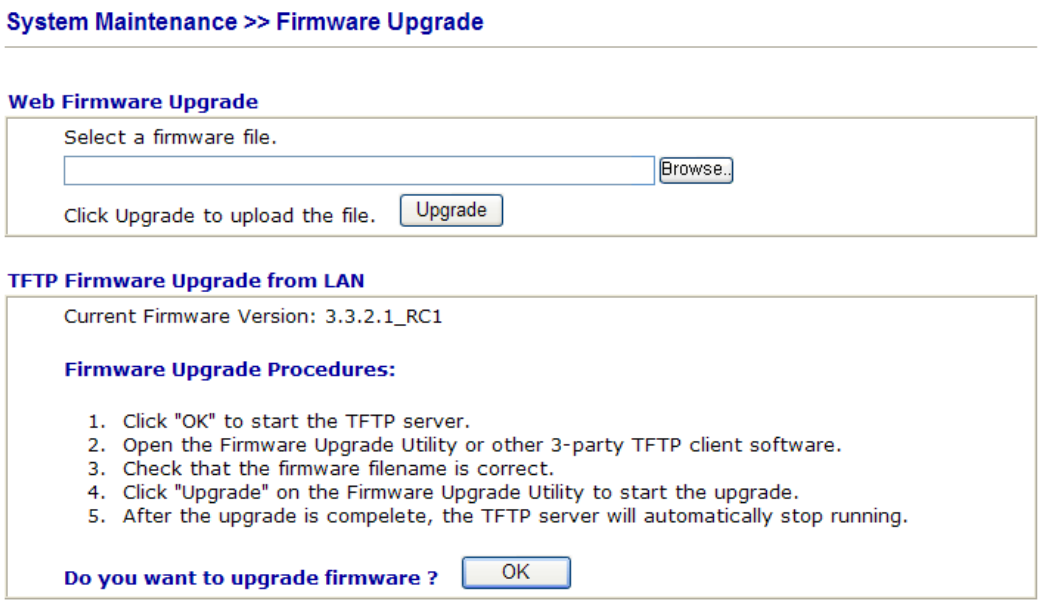
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

3.15.9 Firmware Upgrade

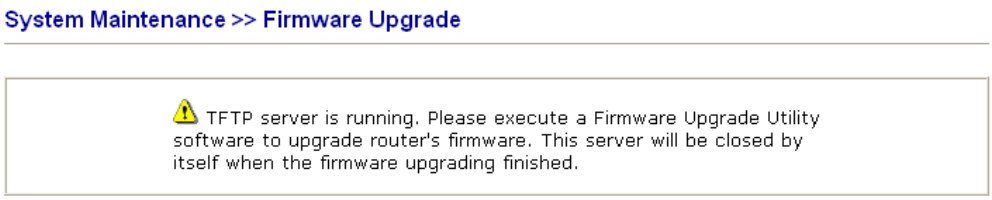
Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.


System Maintenance >> Firmware Upgrade
Web Firmware Upgrade
Select a firmware file.
Browse..
Click Upgrade to upload the file.
Upgrade
TFTP Firmware Upgrade from LAN
Current Firmware Version: 3.3.2.1_RC1
Firmware Upgrade Procedures:
1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is compelete, the TFTP server will automatically stop running.
Do you want to upgrade firmware ?
OK

Click **OK**. The following screen will appear. Please execute the firmware upgrade utility first.

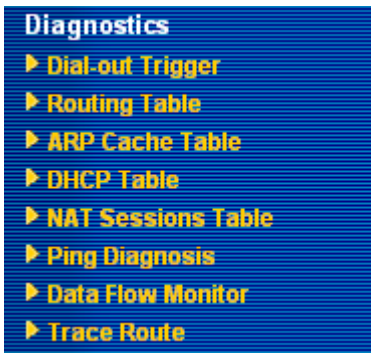

System Maintenance >> Firmware Upgrade
TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

For the detailed information about firmware update, please go to Chapter 4.

3.16 Diagnostics

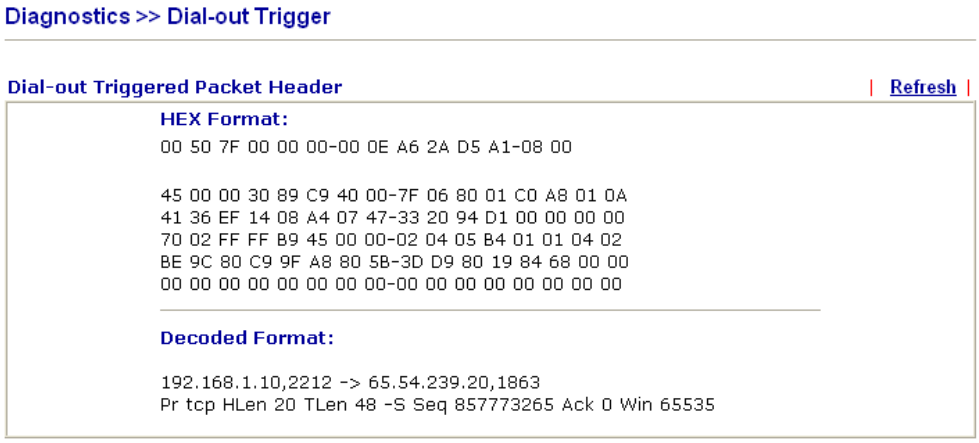
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



3.16.1 Dial-out Trigger

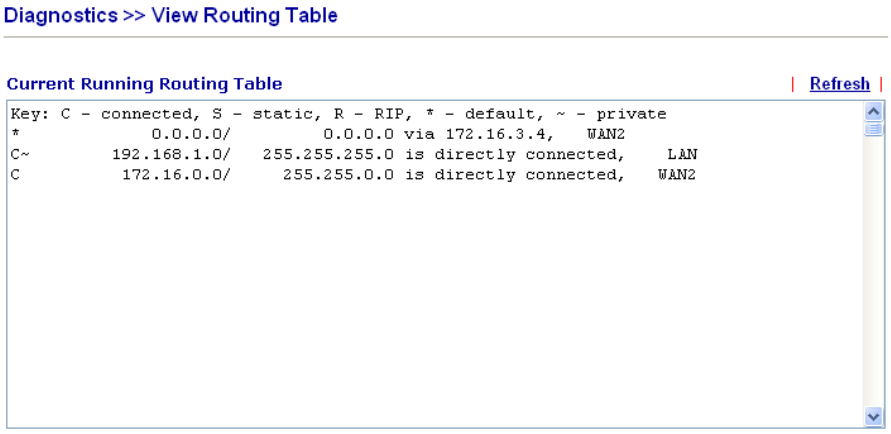
Click **Diagnostics** and click **Dial-out Trigger** to open the web page. The internet connection (e.g., ISDN, PPPoE, PPPoA, etc) is triggered by a package sending from the source IP address.



Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.
Refresh	Click it to reload the page.

3.16.2 Routing Table

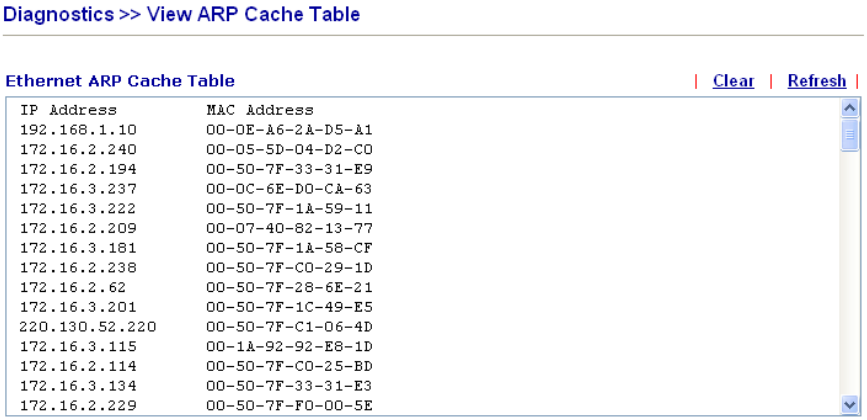
Click **Diagnostics** and click **Routing Table** to open the web page.


Diagnostics >> View Routing Table
Current Running Routing Table
Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private
* 0.0.0.0/ 0.0.0.0 via 172.16.3.4, WAN2
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN
C 172.16.0.0/ 255.255.0.0 is directly connected, WAN2

Refresh	Click it to reload the page.

3.16.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

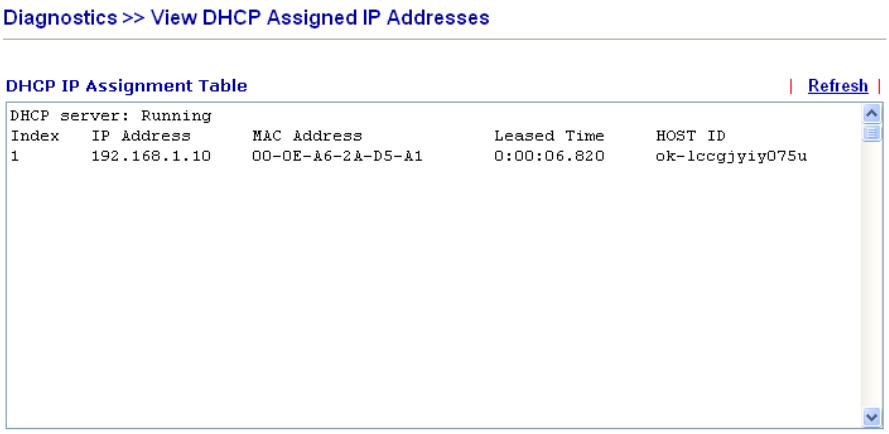


Refresh	Click it to reload the page.
Clear	Click it to clear the whole table.

3.16.4 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

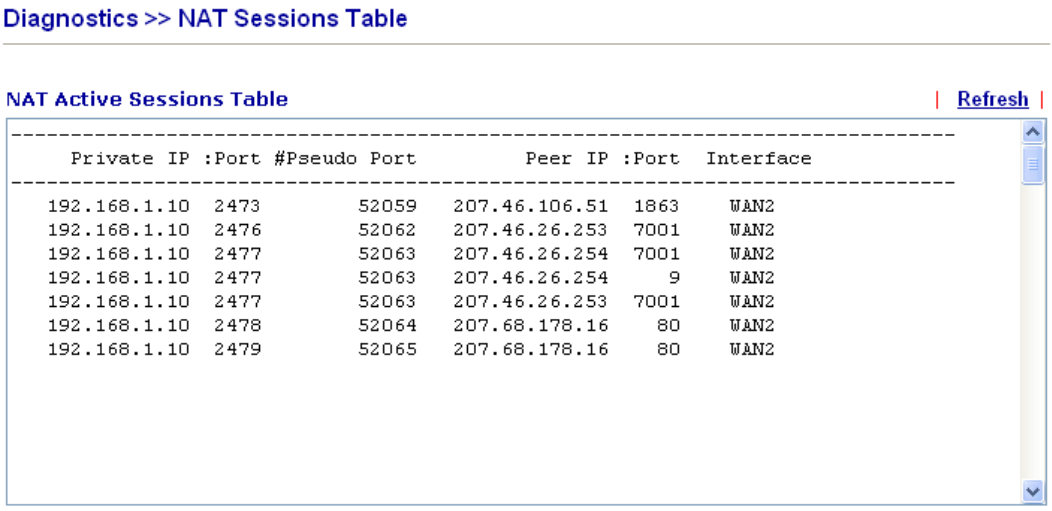
Click **Diagnostics** and click **DHCP Table** to open the web page.


Diagnostics >> View DHCP Assigned IP Addresses
DHCP IP Assignment Table
Refresh
DHCP server: Running
Index IP Address MAC Address Leased Time HOST ID
1 192.168.1.10 00-0E-A6-2A-D5-A1 0:00:06.820 ok-lccgjyiy075u

Index	It displays the connection item number.
IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.
Refresh	Click it to reload the page.

3.16.5 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the setup page.

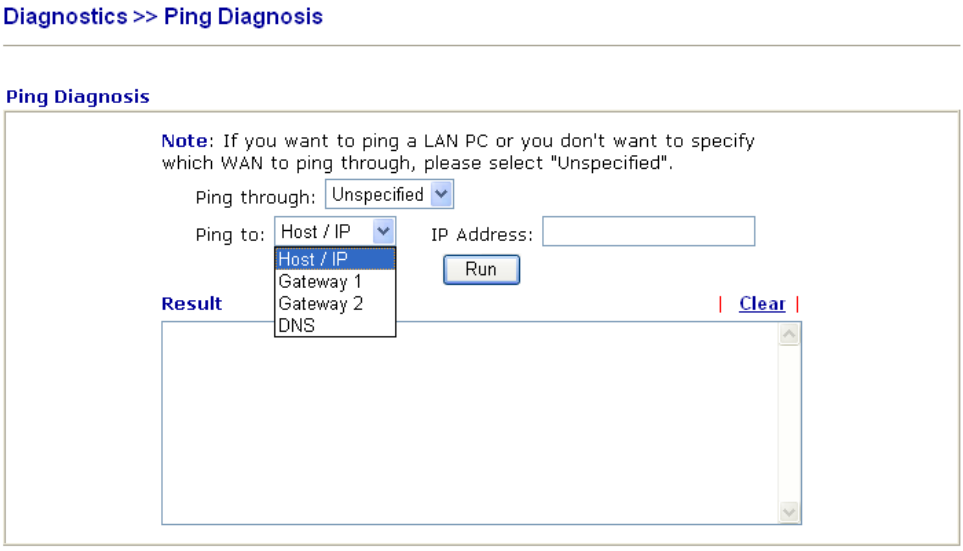


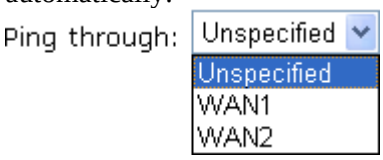
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.

Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

3.16.6 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

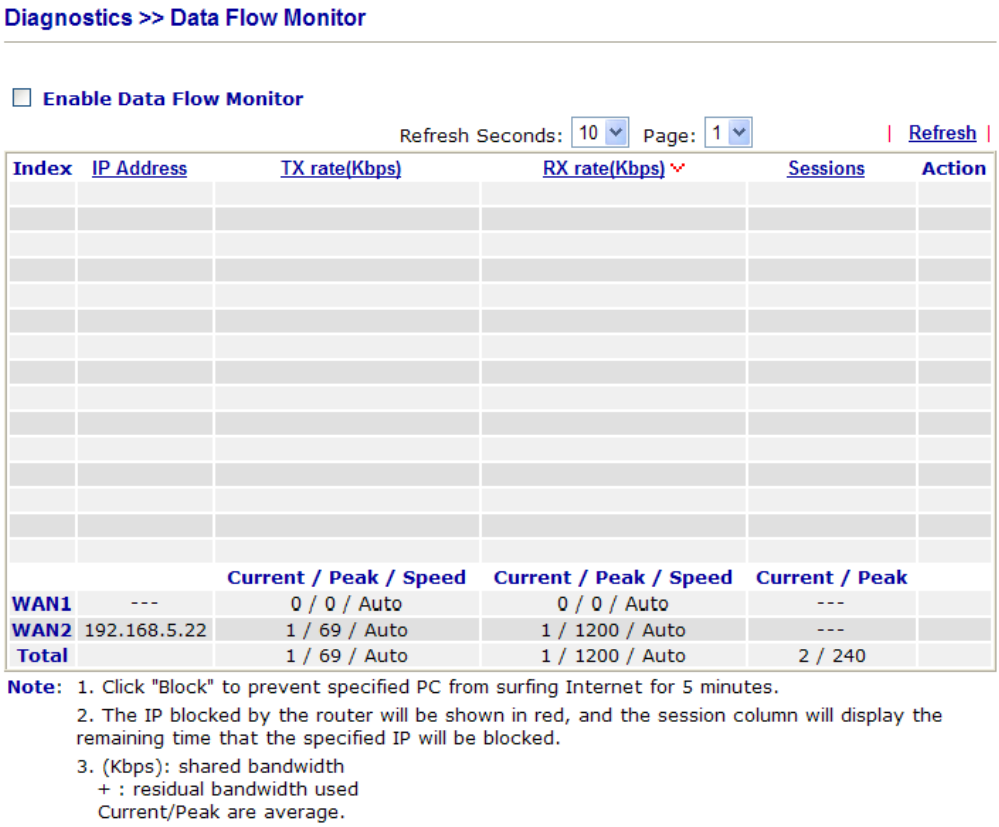


Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically. 
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type in the IP address of the Host/IP that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

3.16.7 Data Flow Monitor

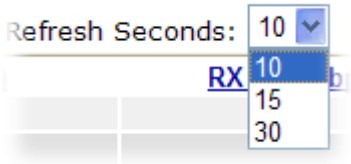
This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.


Diagnostics >> Data Flow Monitor
Enable Data Flow Monitor
Refresh Seconds: 10 Page: 1 | Refresh |
Index IP Address TX rate(Kbps) RX rate(Kbps) Sessions Action
Current / Peak / Speed Current / Peak / Speed Current / Peak
WAN1 --- 0 / 0 / Auto 0 / 0 / Auto ---
WAN2 192.168.5.22 1 / 69 / Auto 1 / 1200 / Auto ---
Total 1 / 69 / Auto 1 / 1200 / Auto 2 / 240
Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.
2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.
3. (Kbps): shared bandwidth
+ : residual bandwidth used
Current/Peak are average.

Enable Data Flow Monitor — Check this box to enable this function.

Refresh Seconds — Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.



Refresh — Click this link to refresh this page manually.

Index — Display the number of the data flow.

IP Address — Display the IP address of the monitored device.

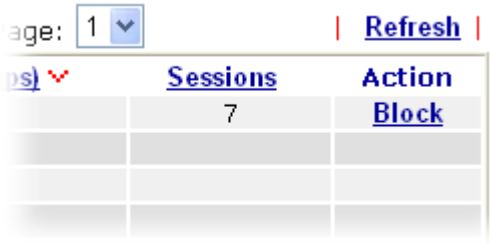
TX rate (kbps) — Display the transmission speed of the monitored device.

RX rate (kbps) — Display the receiving speed of the monitored device.

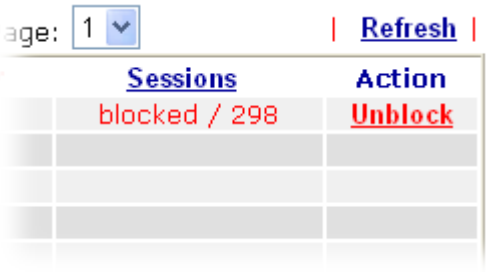
Sessions — Display the session number that you specified in Limit Session web page.

Action

Block - can prevent specified PC accessing into Internet within 5 minutes.

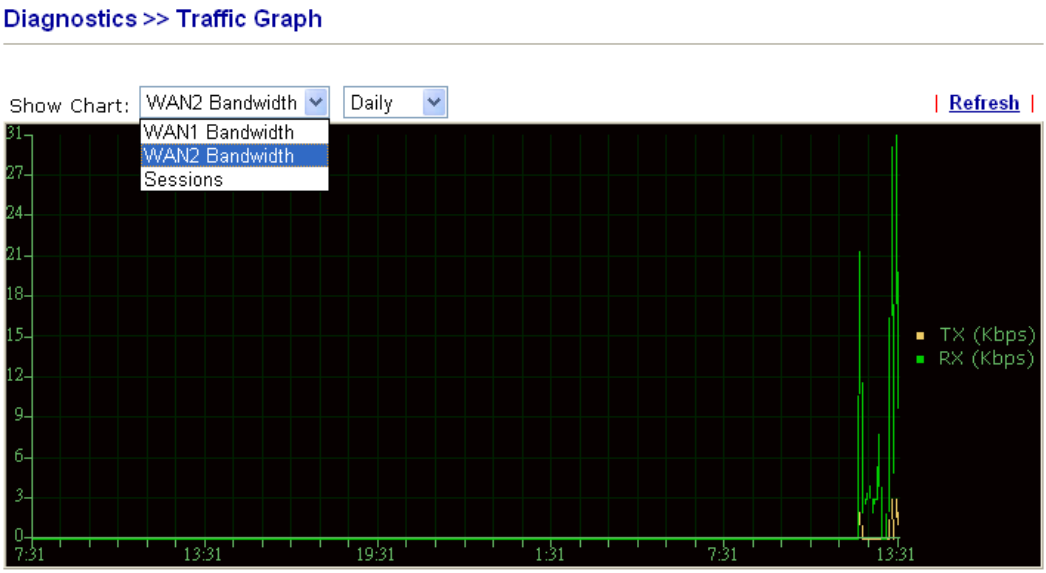


Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.



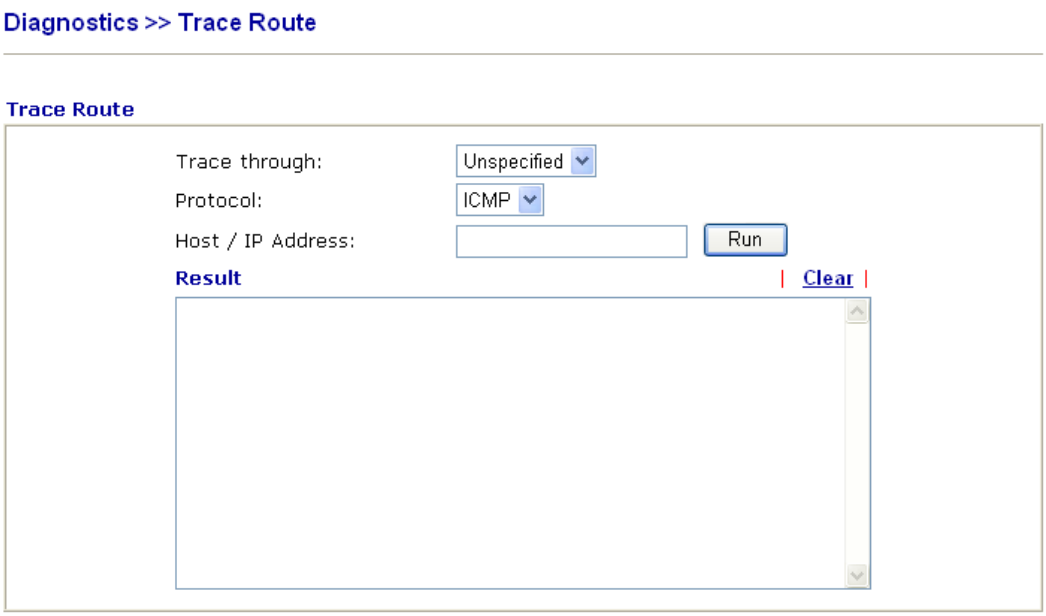
3.16.8 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



3.16.9 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.



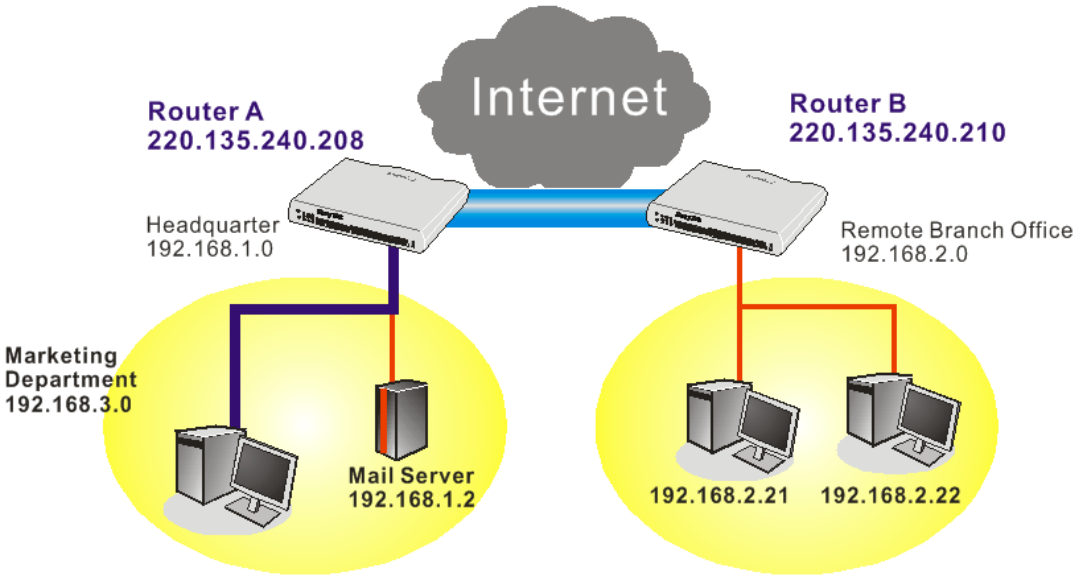
Trace through	Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.
Protocol	Choose a protocol (ICMP or UDP) for such route.
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

This page is left blank.

4 Application and Examples

4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

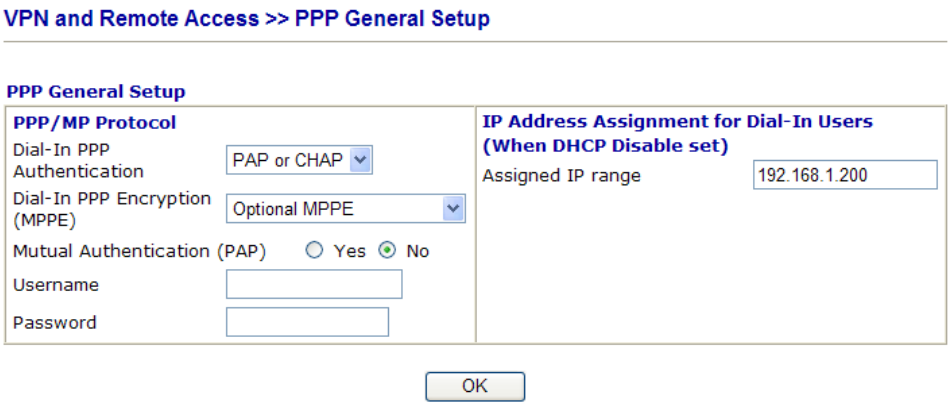
The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.



Settings in Router A in headquarter:

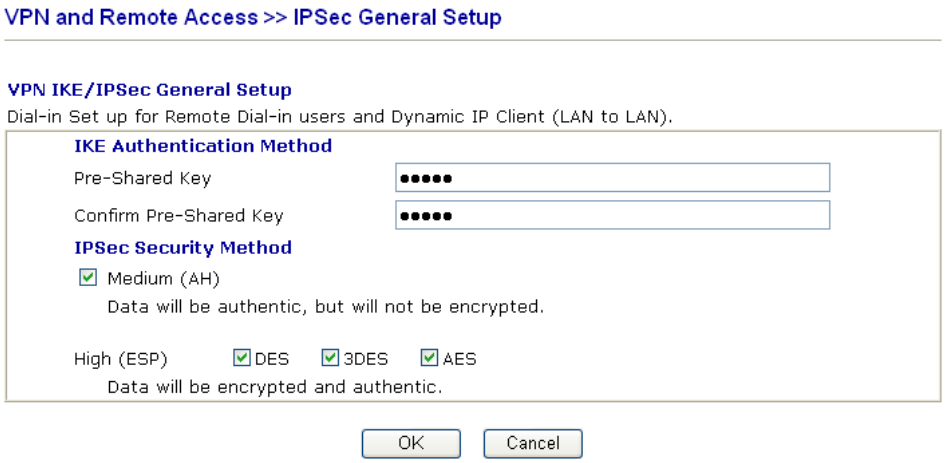
1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.

2. Then,
   For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

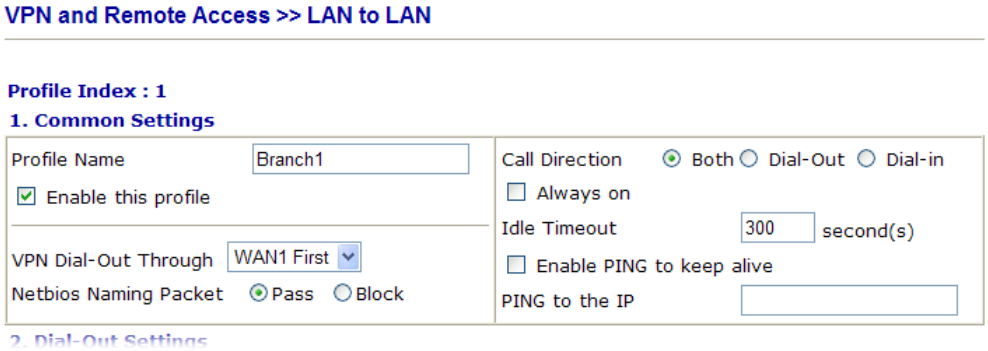


For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set

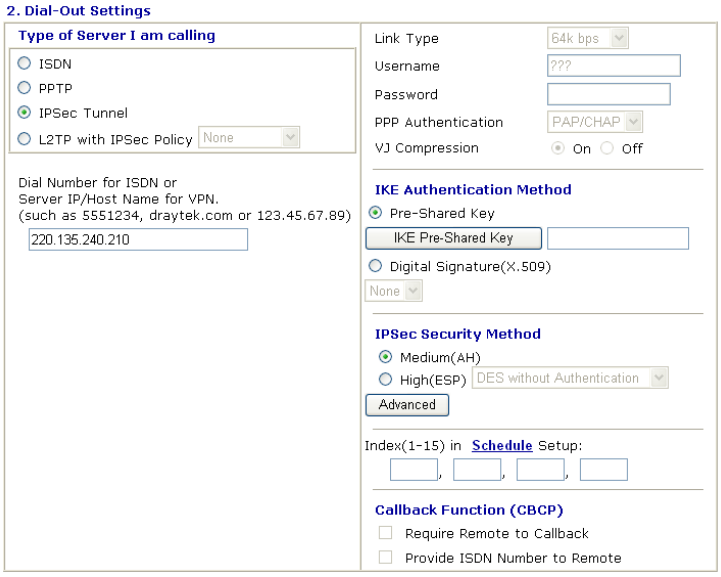
general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.



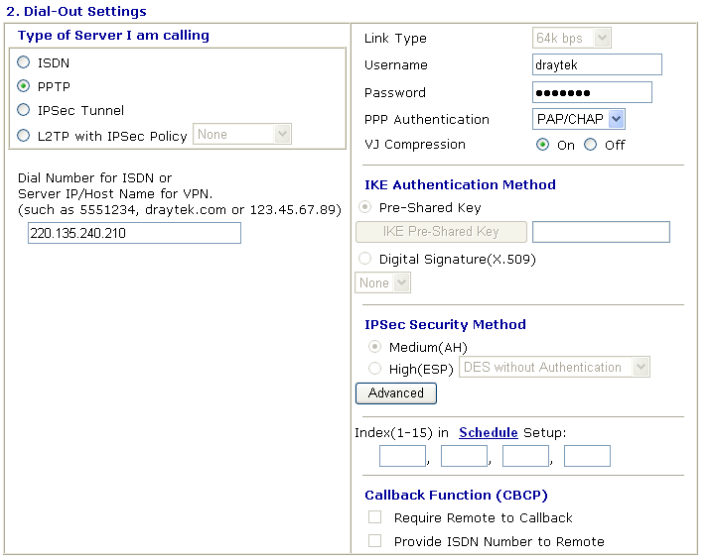
3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.



5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.
   If an ***IPSec-based*** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

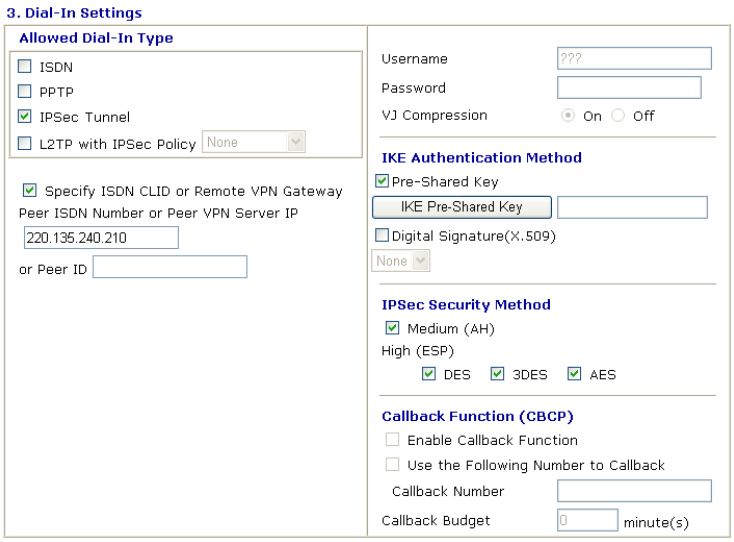


If a ***PPP-based service*** is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

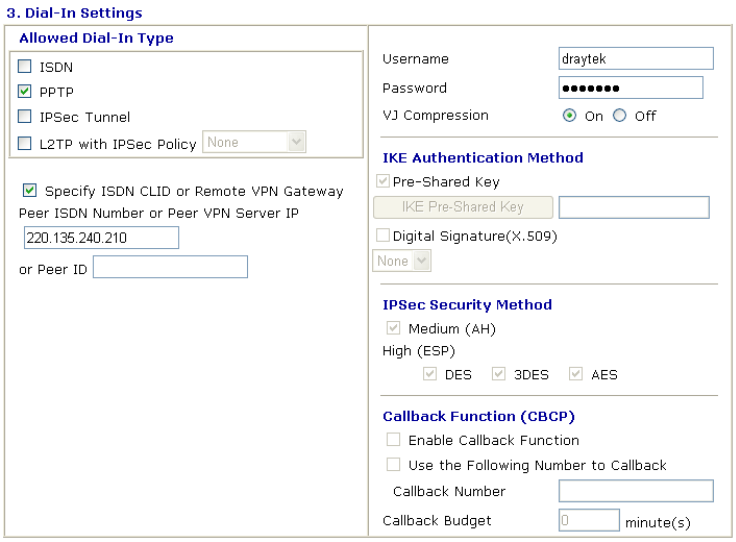


6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

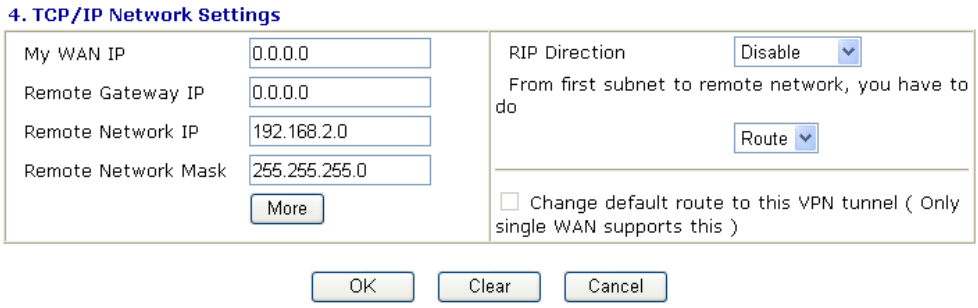
   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



If a ***PPP-based service*** is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



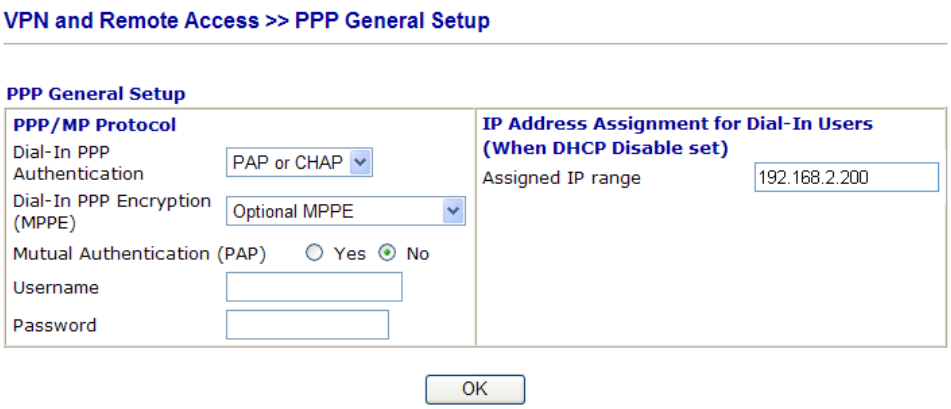
7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.



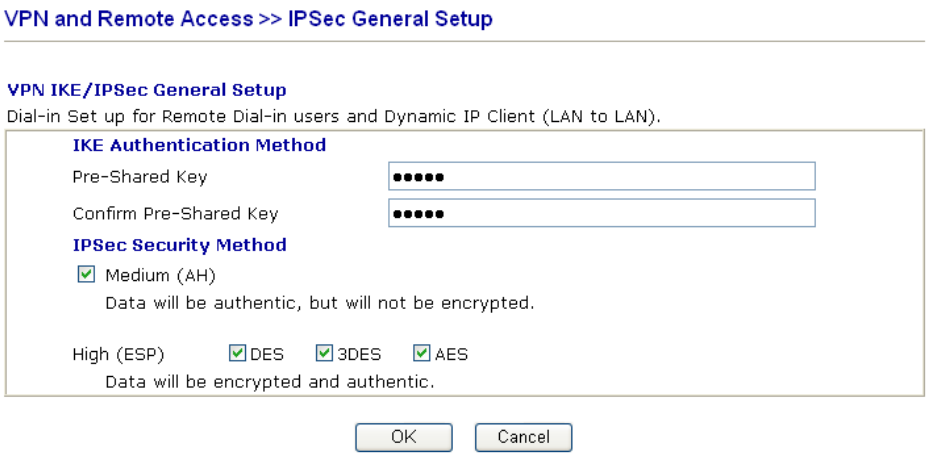
Settings in Router B in the remote office:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.

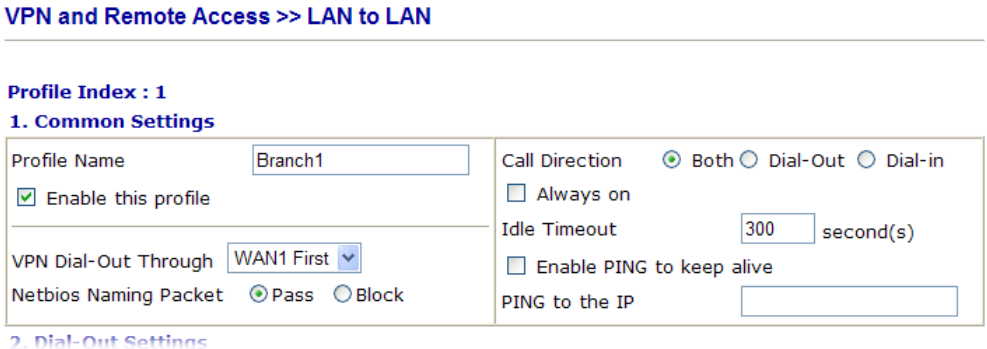
2. Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

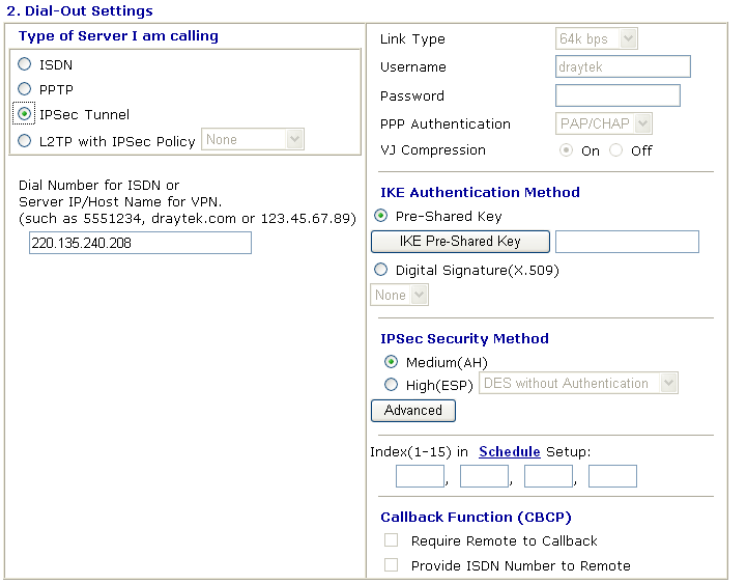


3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

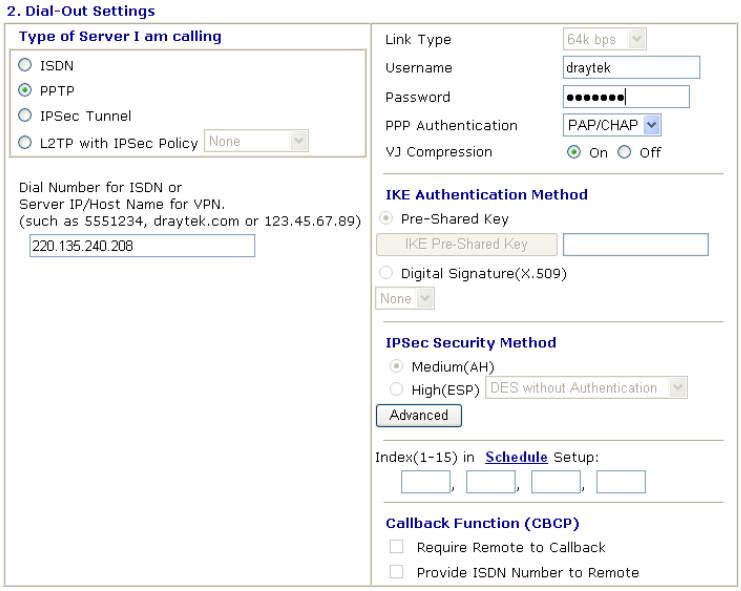


5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an ***IPSec-based*** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

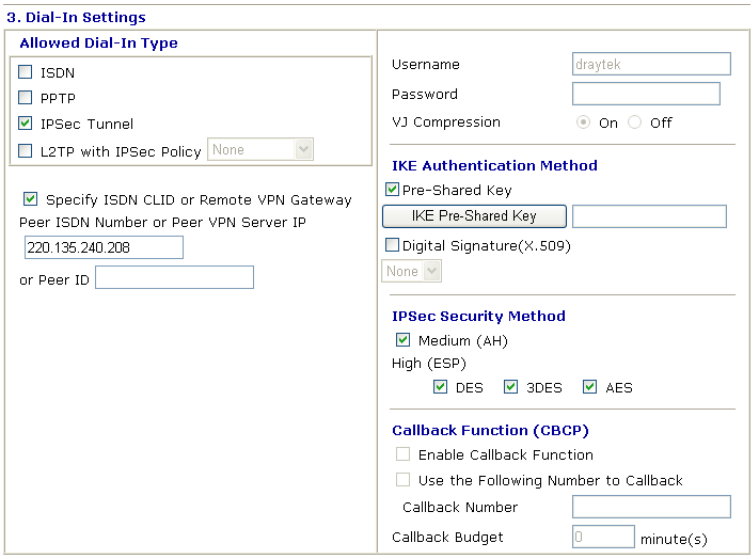


If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

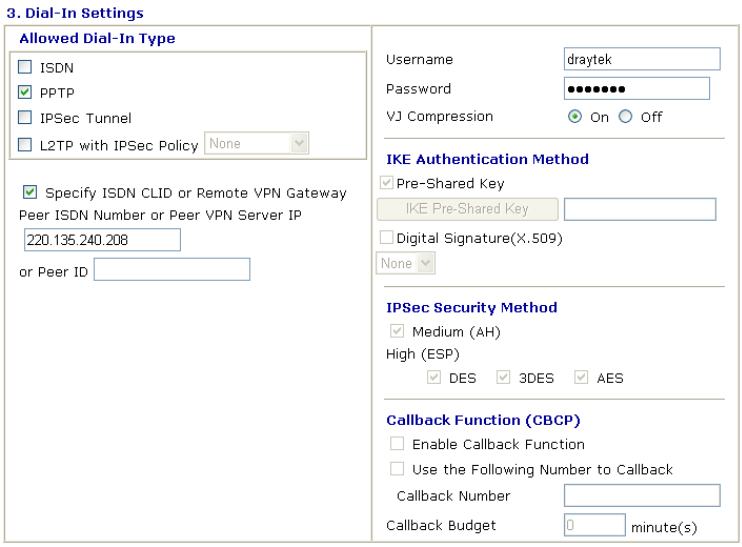


6. Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

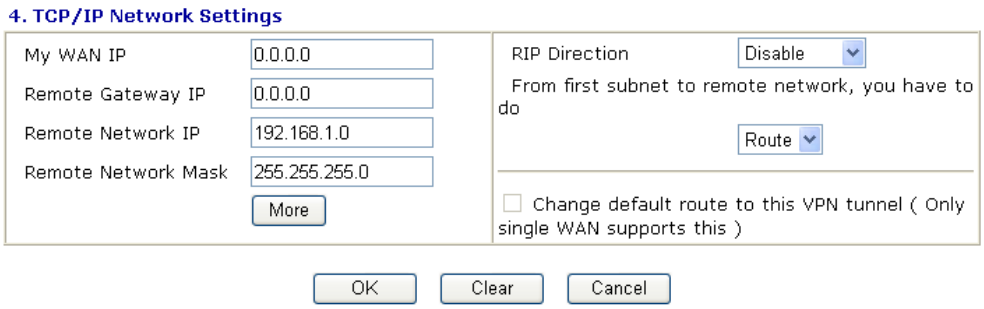
   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

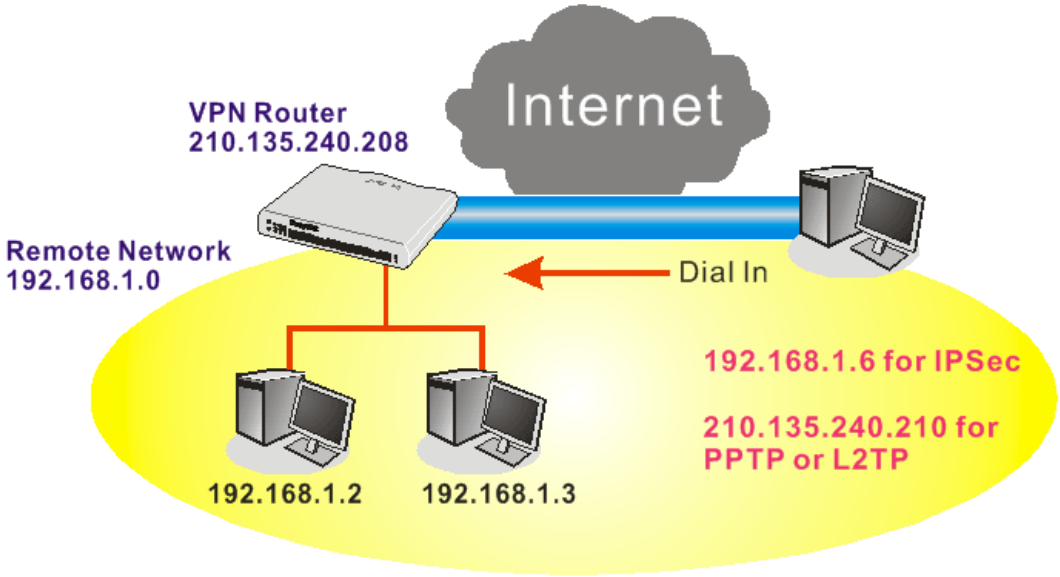


7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.



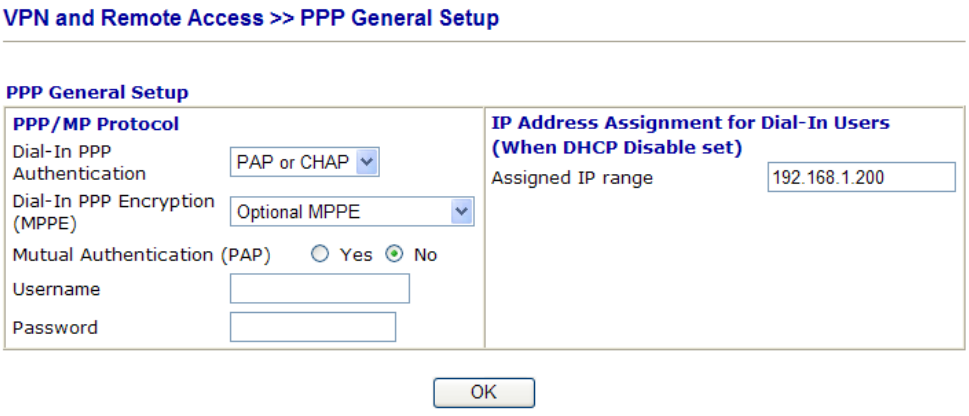
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.

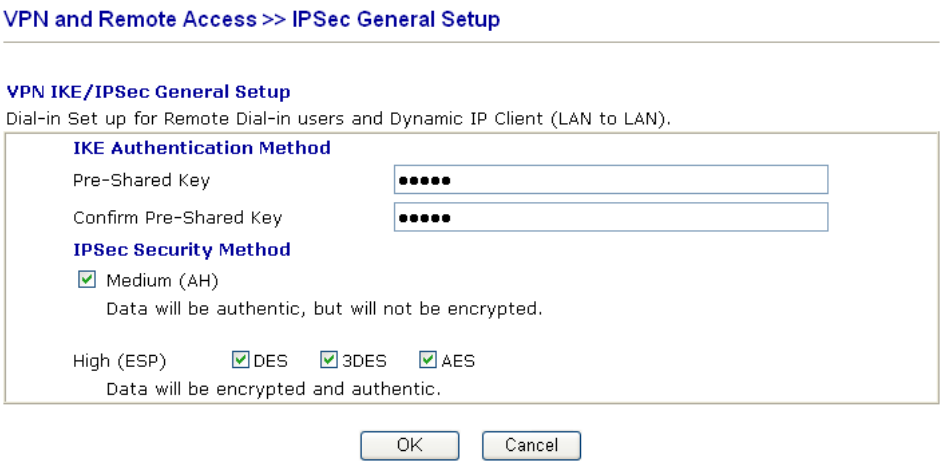


Settings in VPN Router in the enterprise office:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

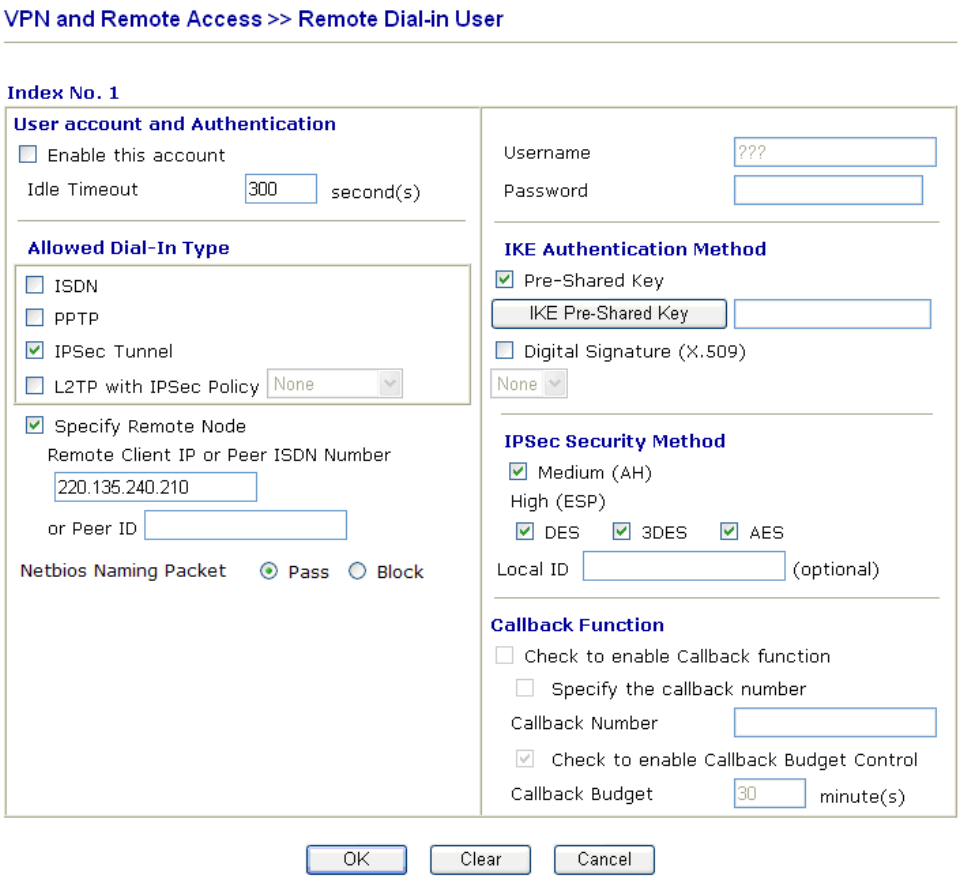


For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.

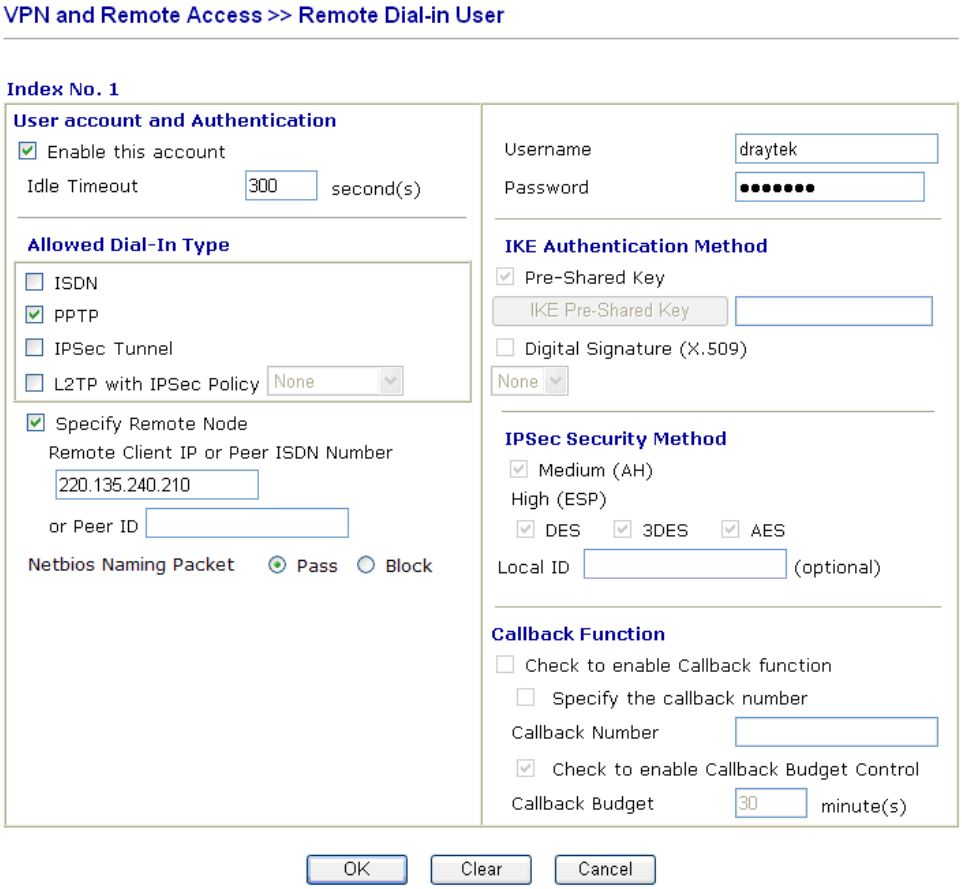


3. Go to **Remote Dial-In User**. Click on one index number to edit a profile.
4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

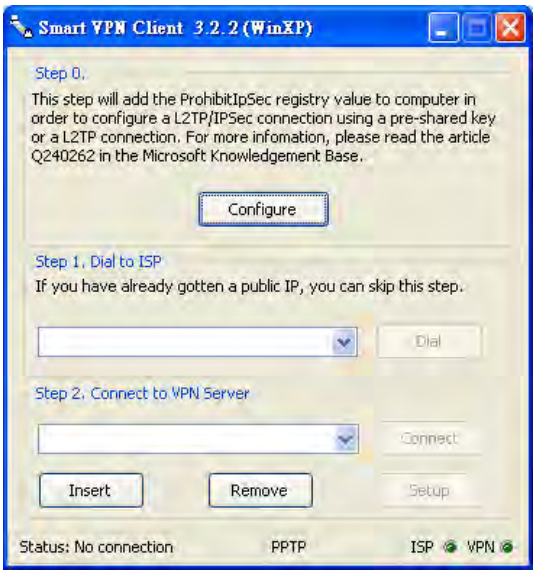


If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



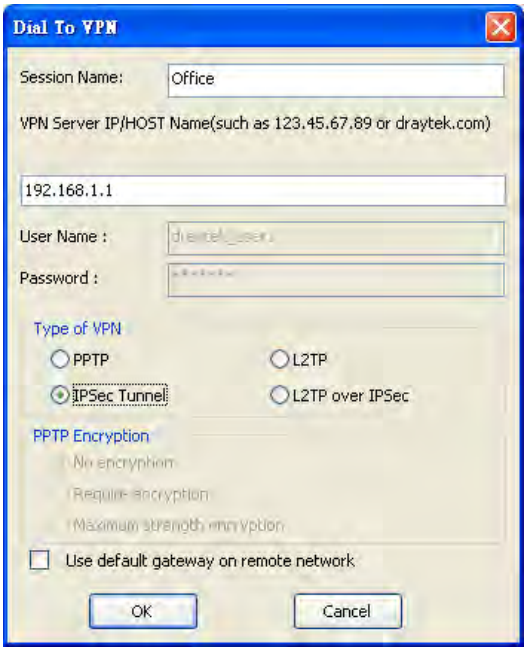
Settings in the remote host:

1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or “Smart VPN Client”, complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or go to www.draytek.com download center. Install as instructed.
2. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.

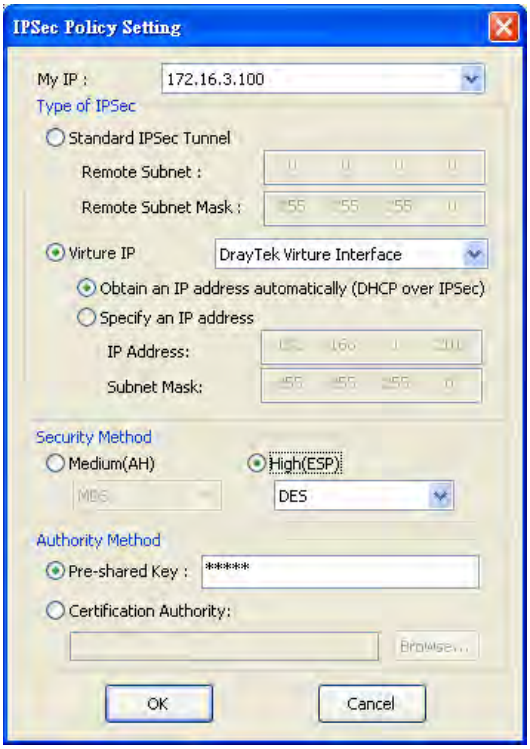

Smart VPN Client 3.2.2 (WinXP)
Step 0.
This step will add the ProhibitIpSec registry value to computer in order to configure a L2TP/IPSec connection using a pre-shared key or a L2TP connection. For more infomation, please read the article Q240262 in the Microsoft Knowledgement Base.
Configure
Step 1. Dial to ISP
If you have already gotten a public IP, you can skip this step.
Dial
Step 2. Connect to VPN Server
Connect
Insert
Remove
Setup
Status: No connection
PPTP
ISP
VPN

3. In **Step 2. Connect to VPN Server**, click **Insert** button to add a new entry.

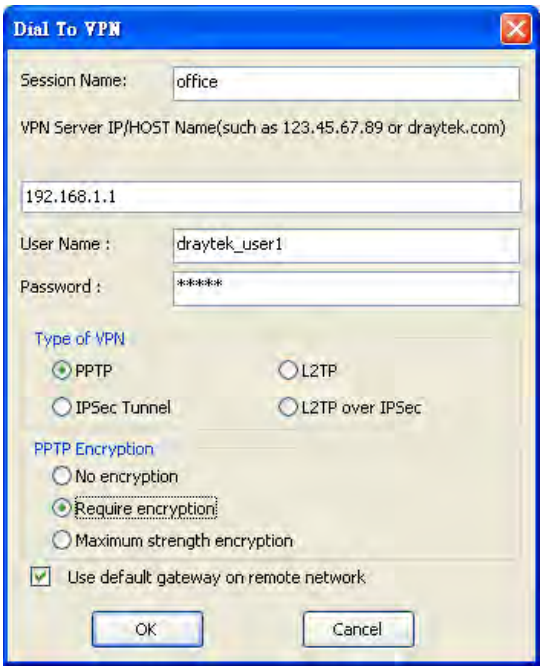
If an IPSec-based service is selected as shown below,



You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.



If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.

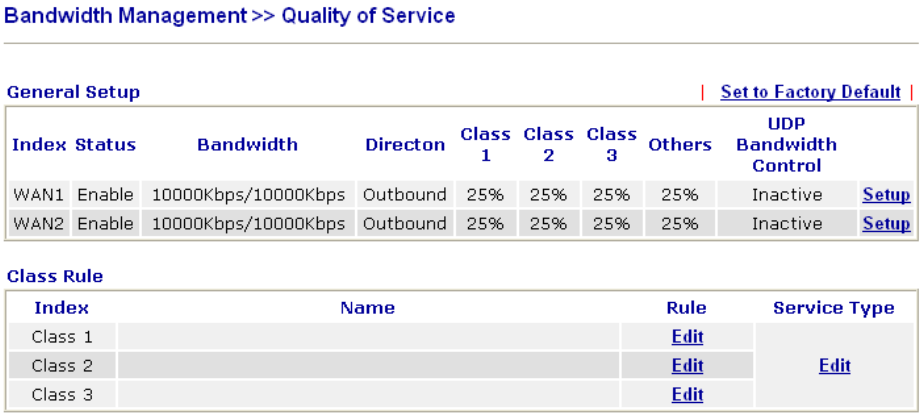


4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

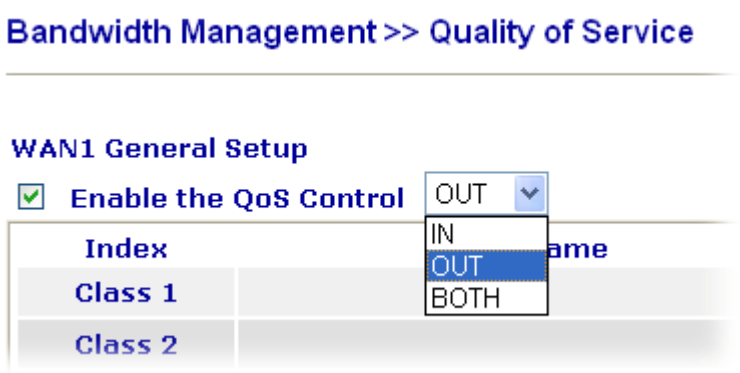
4.3 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

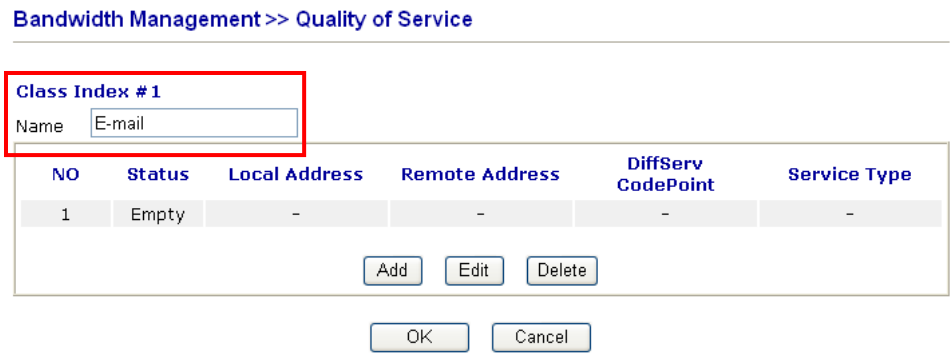
1. Go to **Bandwidth Management>>Quality of Service.**


Bandwidth Management >> Quality of Service
General Setup
Set to Factory Default
Index Status Bandwidth Directon Class 1 Class 2 Class 3 Others UDP Bandwidth Control
WAN1 Enable 10000Kbps/10000Kbps Outbound 25% 25% 25% 25% Inactive Setup
WAN2 Enable 10000Kbps/10000Kbps Outbound 25% 25% 25% 25% Inactive Setup
Class Rule
Index Name Rule Service Type
Class 1 Edit
Class 2 Edit Edit
Class 3 Edit

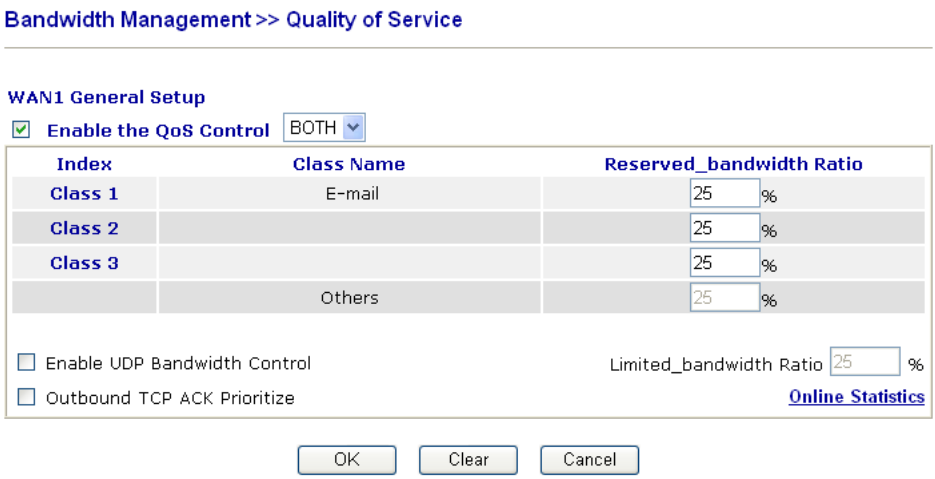
2. Click **Setup** link of WAN 1. Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.



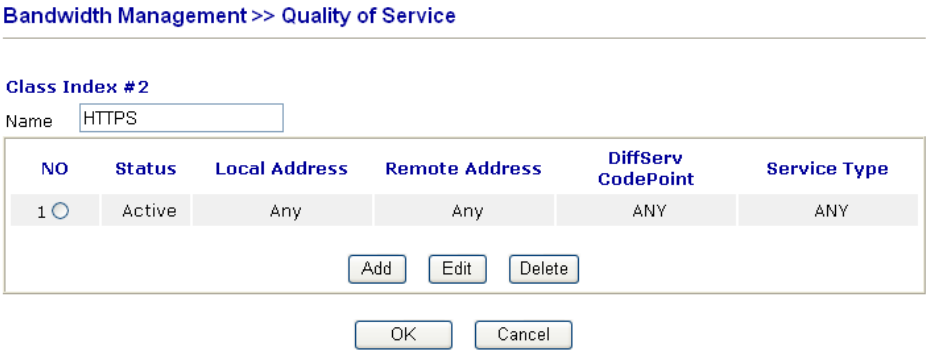
3. Return to previous page. Enter the Name of Index Class 1 by clicking **Edit** link. Type the name "**E-mail**" for Class 1.


Bandwidth Management >> Quality of Service
Class Index #1
Name E-mail
NO Status Local Address Remote Address DiffServ CodePoint Service Type
1 Empty - - - -
Add Edit Delete
OK Cancel

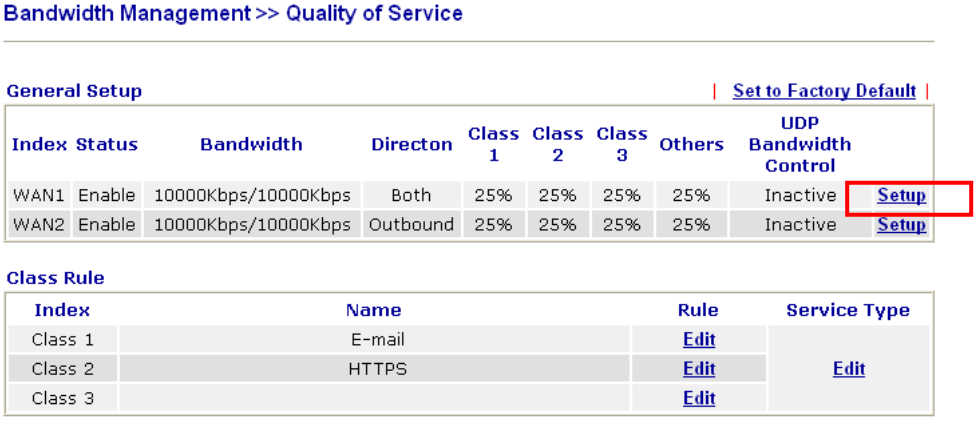
4. For this index, the user will set reserved bandwidth (e.g., 25%) for **E-mail** using protocol POP3 and SMTP.



5. Return to previous page. Enter the Name of Index Class 2 by clicking **Edit** link. In this index, the user will set reserved bandwidth for **HTTPS**. And click **OK**.

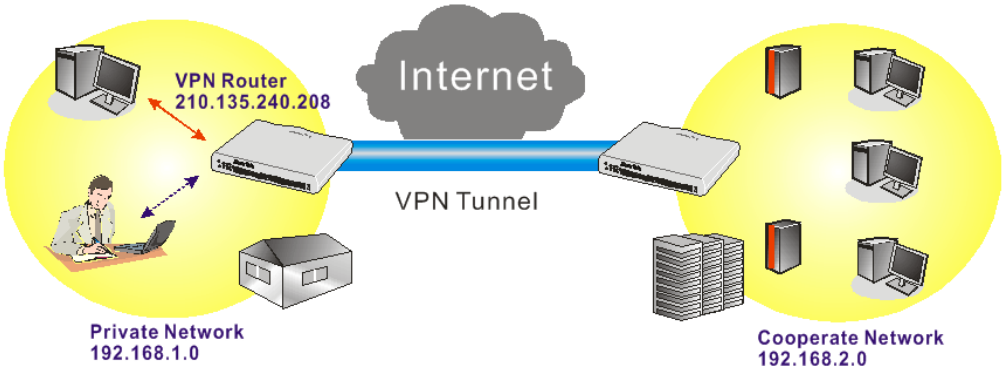


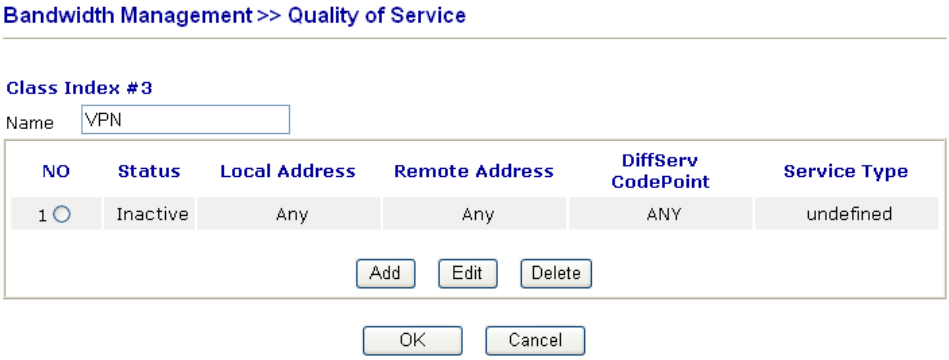
6. Click **Setup** link for WAN1.



7. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic of VoIP influent other application. Click **OK**.

8. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.



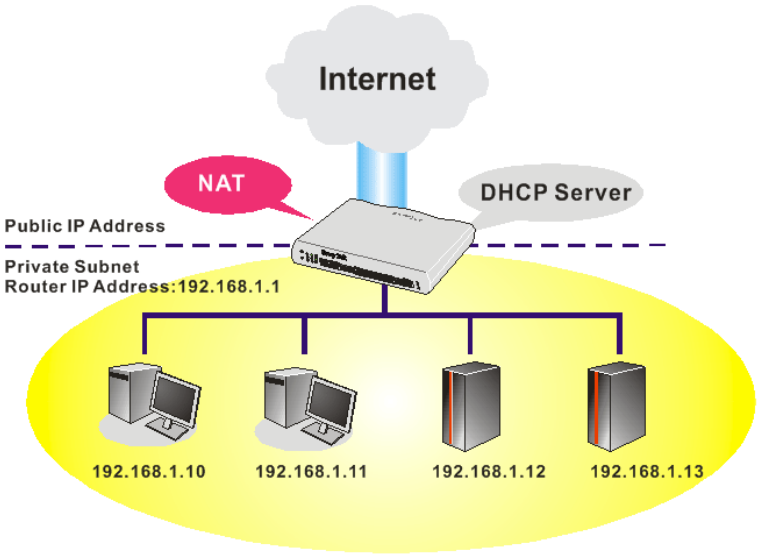


9. Click **Edit** to open the following window. Check the **ACT** box, first.

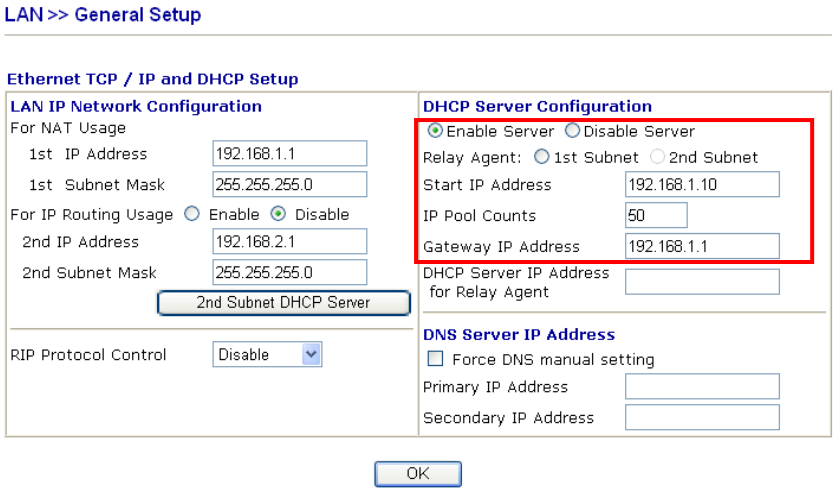
10. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.

4.4 LAN – Created by Using NAT

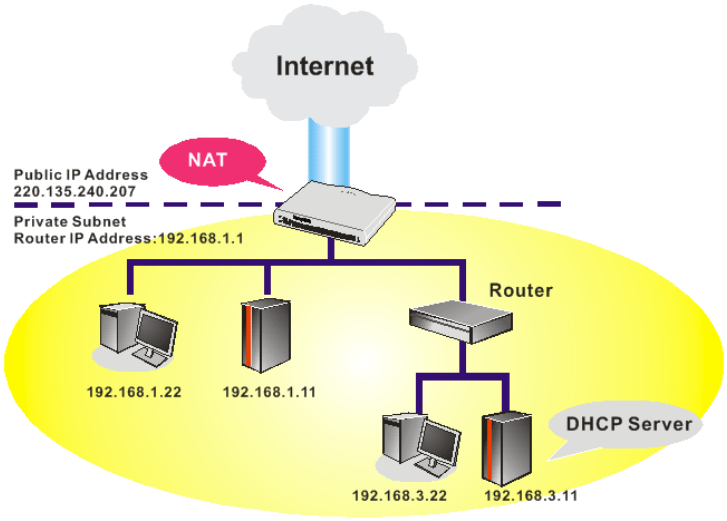
An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



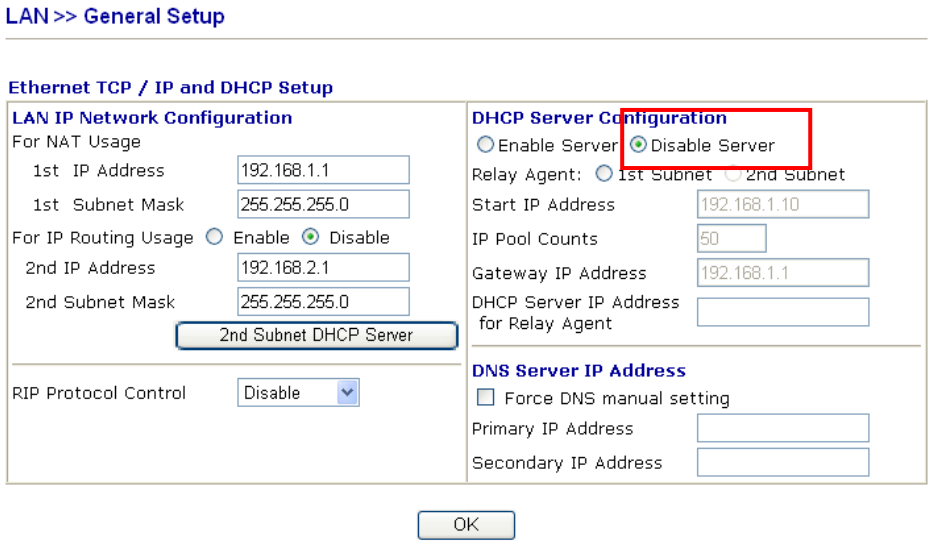
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.


LAN >> General Setup
Ethernet TCP / IP and DHCP Setup
LAN IP Network Configuration
For NAT Usage
1st IP Address 192.168.1.1
1st Subnet Mask 255.255.255.0
For IP Routing Usage Enable Disable
2nd IP Address 192.168.2.1
2nd Subnet Mask 255.255.255.0
2nd Subnet DHCP Server
RIP Protocol Control Disable
DHCP Server Configuration
Enable Server Disable Server
Relay Agent: 1st Subnet 2nd Subnet
Start IP Address 192.168.1.10
IP Pool Counts 50
Gateway IP Address 192.168.1.1
DHCP Server IP Address for Relay Agent
DNS Server IP Address
Force DNS manual setting
Primary IP Address
Secondary IP Address
OK

To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as show below.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.


LAN >> General Setup
Ethernet TCP / IP and DHCP Setup
LAN IP Network Configuration
For NAT Usage
1st IP Address 192.168.1.1
1st Subnet Mask 255.255.255.0
For IP Routing Usage Enable Disable
2nd IP Address 192.168.2.1
2nd Subnet Mask 255.255.255.0
2nd Subnet DHCP Server
RIP Protocol Control Disable
DHCP Server Configuration
Enable Server Disable Server
Relay Agent: 1st Subnet 2nd Subnet
Start IP Address 192.168.1.10
IP Pool Counts 50
Gateway IP Address 192.168.1.1
DHCP Server IP Address for Relay Agent
DNS Server IP Address
Force DNS manual setting
Primary IP Address
Secondary IP Address
OK

4.5 Calling Scenario for VoIP function

4.5.1 Calling via SIP Sever

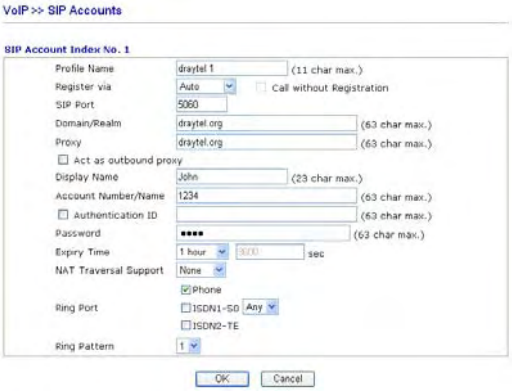
Example 1: Both John and David have SIP Addresses from different service providers.

John's SIP URL: 1234@draytel.org, David's SIP URL: 4321@iptel.org

Settings for John
DialPlan index 1
Phone Number: 1111
Display Name: David
SIP URL: 4321@iptel.org

SIP Accounts Settings ---

Profile Name: draytel1
Register via: Auto
SIP Port: 5060 (default)
Domain/Realm: draytel.org
Proxy: draytel.org
Act as outbound proxy: unhecked
Display Name: John
Account Number/Name: 1234
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

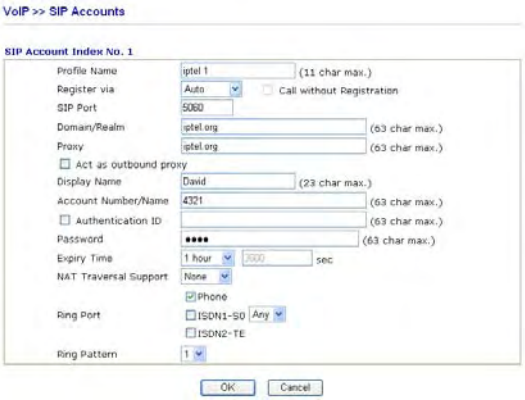

VoIP >> SIP Accounts
SIP Account Index No. 1
Profile Name draytel 1 (11 char max.)
Register via Auto Call without Registration
SIP Port 5060
Domain/Realm draytel.org (63 char max.)
Proxy draytel.org (63 char max.)
Act as outbound proxy
Display Name John (23 char max.)
Account Number/Name 1234 (63 char max.)
Authentication ID (63 char max.)
Password (63 char max.)
Expiry Time 1 hour sec
NAT Traversal Support None
Phone
Ring Port ISDN1-S0 Any
ISDN2-TE
Ring Pattern 1
OK Cancel

CODEC/RTP/DTMF ---
(Use default value)

John calls David ---
He picks up the phone and dials 1111#. (DialPlan Phone Number for David)

Settings for David
DialPlan index 1
Phone Number:2222
Display Name: John
SIP URL:1234@draytel.org

SIP Accounts Settings ---
Profile Name: iptel 1
Register via: Auto
SIP Port: 5060(default)
Domain/Realm: iptel.org
Proxy: iptel.org
Act as outbound proxy: unchecked
Display Name: David
Account Name: 4321
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)


VoIP >> SIP Accounts
SIP Account Index No. 1
Profile Name iptel 1 (11 char max.)
Register via Auto Call without Registration
SIP Port 5060
Domain/Realm iptel.org (63 char max.)
Proxy iptel.org (63 char max.)
Act as outbound proxy
Display Name David (23 char max.)
Account Number/Name 4321 (63 char max.)
Authentication ID (63 char max.)
Password (63 char max.)
Expiry Time 1 hour sec
NAT Traversal Support None
Phone
Ring Port ISDN1-S0 Any
ISDN2-TE
Ring Pattern 1
OK Cancel

CODEC/RTP/DTMF ---
(Use default value)

David calls John
He picks up the phone and dials 2222# (DialPlan Phone Number for John)

Example 2: Both John and David have SIP Addresses from the same service provider.

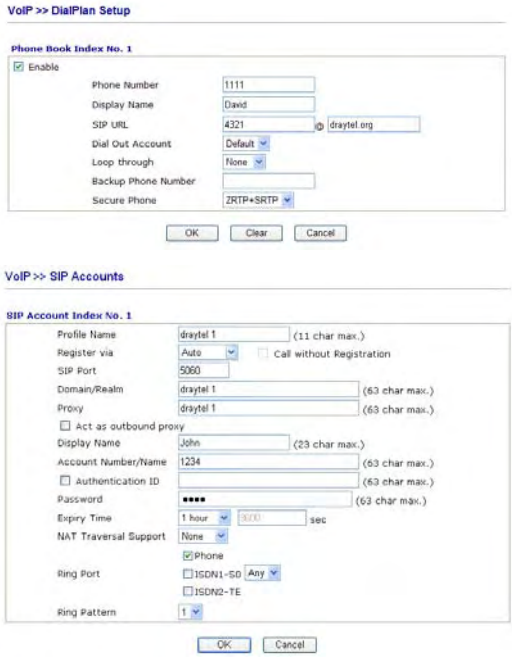
John's SIP URL: 1234@draytel.org , David's SIP URL: 4321@draytel.org

Settings for John
DialPlan index 1
Phone Number: 1111
Display Name: David
SIP URL: 4321@draytel.org

SIP Accounts Settings ---

Profile Name: draytel 1
Register via: Auto
SIP Port: 5060 (default)
Domain/Realm: draytel.org
Proxy: draytel.org
Act as outbound proxy: unchecked
Display Name: John
Account Number/Name: 1234
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

CODEC/RTP/DTMF ---
(Use default value)

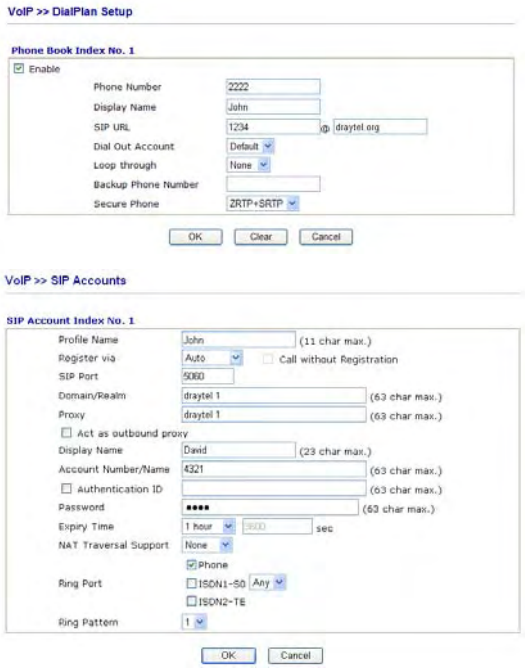

VoIP >> DialPlan Setup
Phone Book Index No. 1
Enable
Phone Number 1111
Display Name David
SIP URL 4321 @ draytel.org
Dial Out Account Default
Loop through None
Backup Phone Number
Secure Phone ZRTP+SRTP
OK Clear Cancel
VoIP >> SIP Accounts
SIP Account Index No. 1
Profile Name draytel 1 (11 char max.)
Register via Auto Call without Registration
SIP Port 5060
Domain/Realm draytel 1 (63 char max.)
Proxy draytel 1 (63 char max.)
Act as outbound proxy
Display Name John (23 char max.)
Account Number/Name 1234 (63 char max.)
Authentication ID (63 char max.)
Password **** (63 char max.)
Expiry Time 1 hour sec
NAT Traversal Support None
Phone
Ring Port ISDN1-S0 Any
ISDN2-TE
Ring Pattern 1
OK Cancel

John calls David
He picks up the phone and dials 1111#. (DialPlan Phone Number for David) Or,
He picks up the phone and dials 4321#. (David's Account Name)

Settings for David
DialPlan index 1
Phone Number:2222
Display Name: John
SIP URL:1234@draytel.org

SIP Accounts Settings ---
Profile Name: John
Register via: Auto
SIP Port: 5060(default)
Domain/Realm: draytel.org
Proxy: iptel.org
Act as outbound proxy: unchecked
Display Name: David
Account Name: 4321
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

CODEC/RTP/DTMF---
(Use default value)


VoIP >> DialPlan Setup
Phone Book Index No. 1
Enable
Phone Number 2222
Display Name John
SIP URL 1234 @ draytel.org
Dial Out Account Default
Loop through None
Backup Phone Number
Secure Phone ZRTP+SRTP
OK Clear Cancel
VoIP >> SIP Accounts
SIP Account Index No. 1
Profile Name John (11 char max.)
Register via Auto Call without Registration
SIP Port 5060
Domain/Realm draytel 1 (63 char max.)
Proxy draytel 1 (63 char max.)
Act as outbound proxy
Display Name David (23 char max.)
Account Number/Name 4321 (63 char max.)
Authentication ID (63 char max.)
Password **** (63 char max.)
Expiry Time 1 hour sec
NAT Traversal Support None
Phone
Ring Port ISDN1-S0 Any
ISDN2-TE
Ring Pattern 1
OK Cancel

David calls John
He picks up the phone and dials 2222# (DialPlan Phone Number for John) Or,
He picks up the phone and dials 1234# (John's Account Name)

4.5.2 Peer-to-Peer Calling

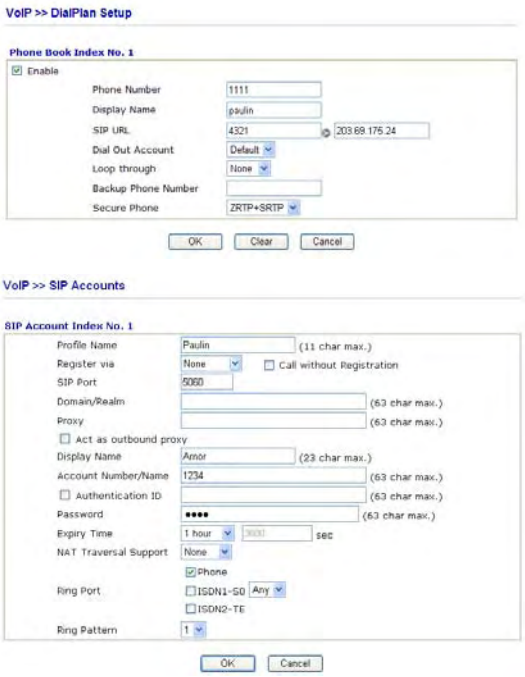
Example 3: Arnor and Paulin have Vigor routers respectively, they can call each other *without* SIP Registrar. First they must have each other's IP address and assign an Account Name for the port used for calling.

Arnor's SIP URL: 1234@214.61.172.53 Paulin's SIP URL: 4321@ 203.69.175.24

Settings for Arnor
DialPlan index 1
Phone Number: 1111
Display Name: paulin
SIP URL: 4321@ 203.69.175.24

SIP Accounts Settings ---
Profile Name: Paulin
Register via: None
SIP Port: 5060(default)
Domain/Realm: (blank)
Proxy: (blank)
Act as outbound proxy: unchecked
Display Name: Arnor
Account Name: 1234
Authentication ID: unchecked
Password: (blank)
Expiry Time: (use default value)

CODEC/RTP/DTMF---
(Use default value)

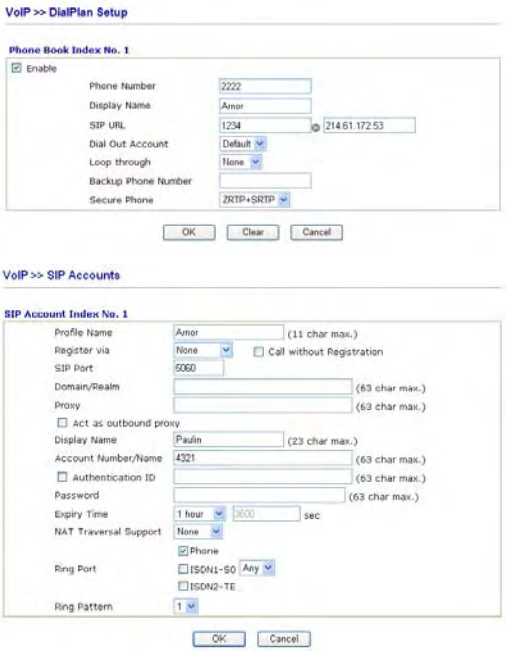


Arnor calls Paulin
He picks up the phone and dials **1111#**. (DialPlan Phone Number for Arnor)

Settings for Paulin
DialPlan index 1
Phone Number:2222
Display Name: Arnor
SIP URL: 1234@214.61.172.53

SIP Accounts Settings ---
Profile Name: Arnor
Register via: None
SIP Port: 5060(default)
Domain/Realm: (blank)
Proxy: (blank)
Act as outbound proxy: unchecked
Display Name: Paulin
Account Name: 4321
Authentication ID: unchecked
Password: (blank)
Expiry Time: (use default value)

CODEC/RTP/DTMF---
(Use default value)

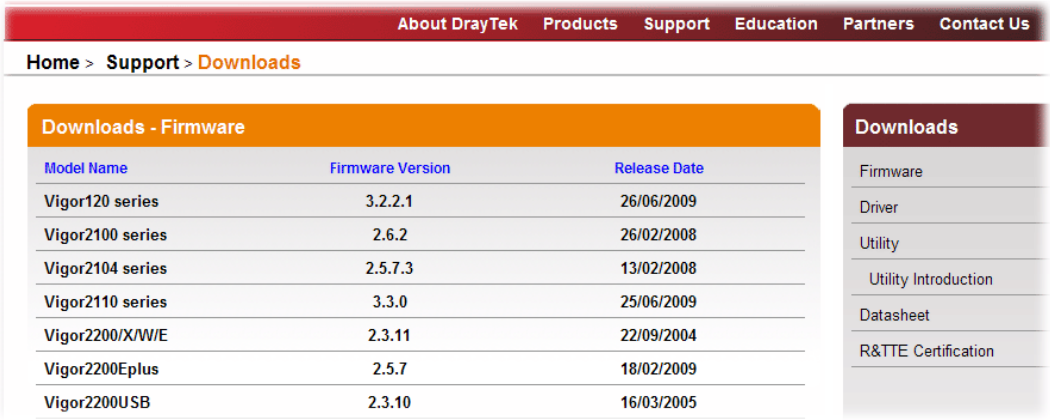


Paulin calls Arnor
He picks up the phone and dials **2222#** (DialPlan Phone Number for John)

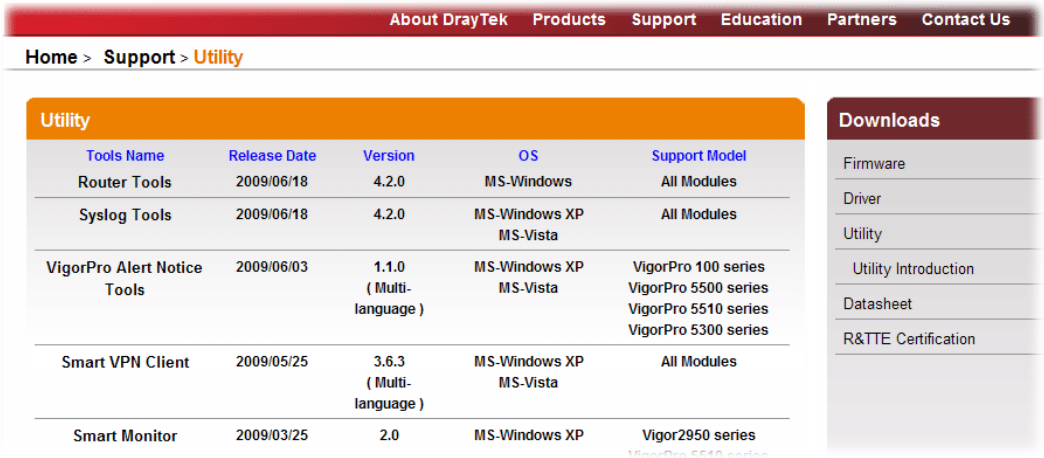
4.6 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.

1. Go to **www.draytek.com.**
2. Access into **Support >> Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.



3. Access into **Support >> Downloads**. Please find out **Utility** menu and click it.



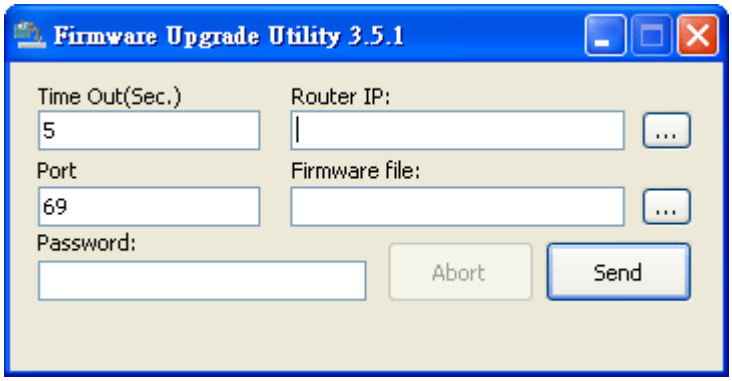
4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

5. Double click on the router tool icon. The setup wizard will appear.

Setup - DrayTek Router Tools V4.2.0
Welcome to the DrayTek Router Tools V4.2.0 Setup Wizard
This will install DrayTek Router Tools V4.2.0 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

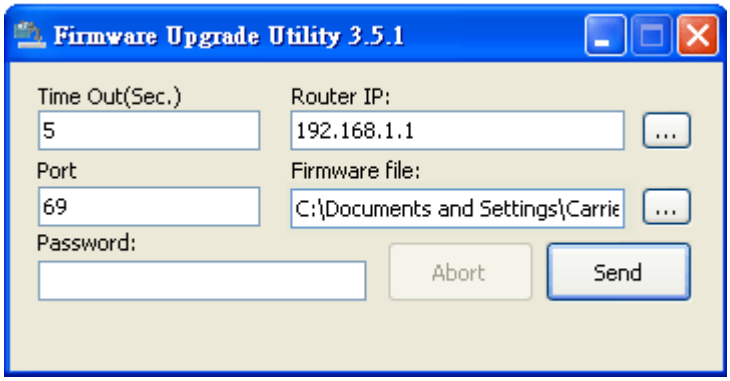
6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.

7. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.

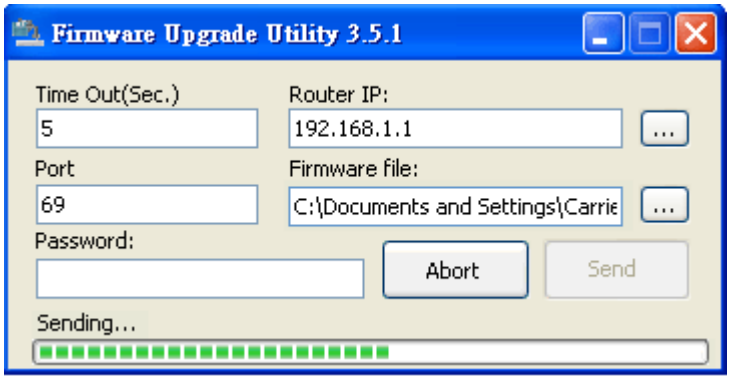


8. Type in your router IP, usually **192.168.1.1**.

9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

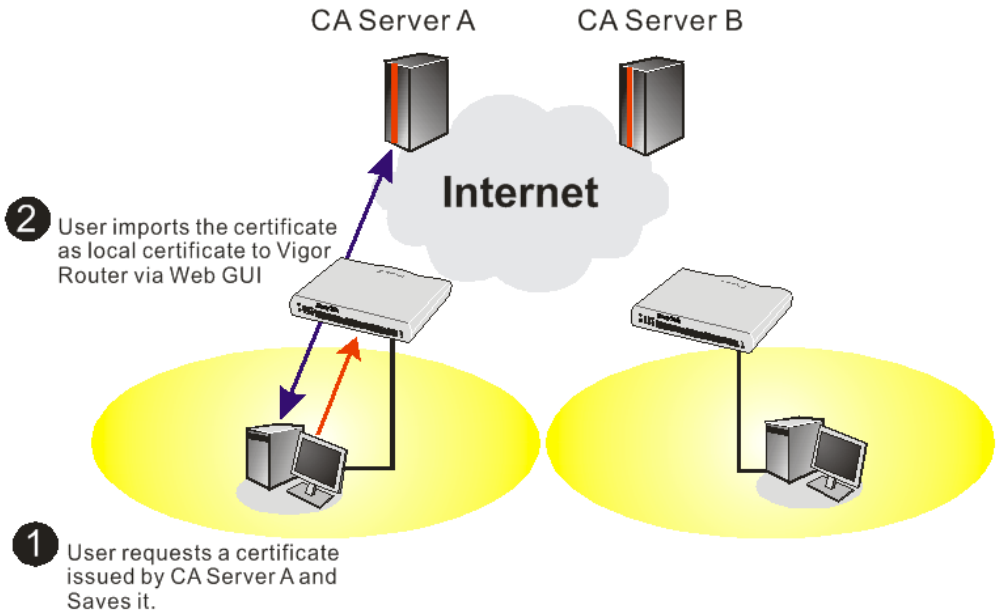


10. Click **Send**.



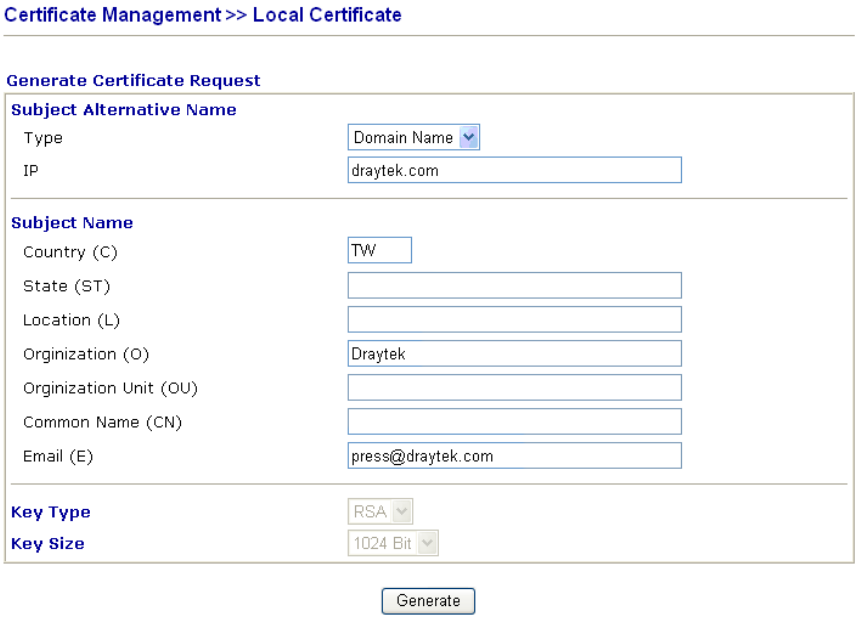
11. Now the firmware update is finished.

4.7 Request a certificate from a CA server on Windows CA Server

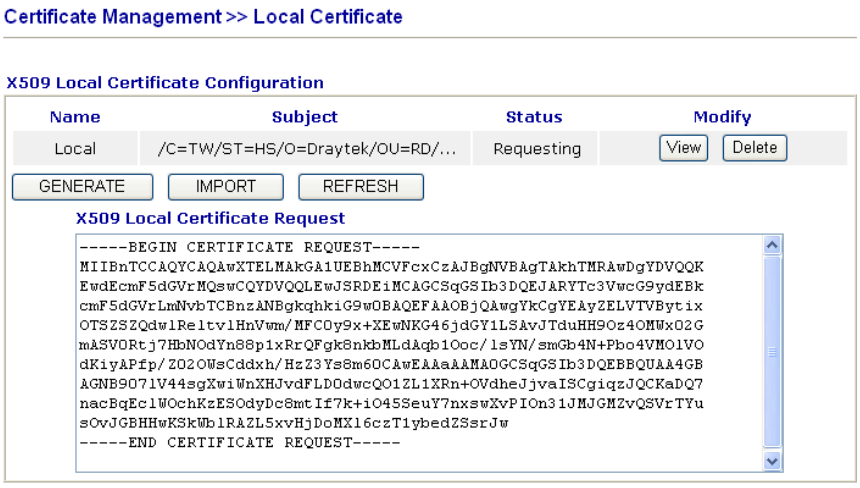

CA Server A
CA Server B
Internet
2
User imports the certificate as local certificate to Vigor Router via Web GUI
1
User requests a certificate issued by CA Server A and Saves it.

1. Go to **Certificate Management** and choose **Local Certificate**.

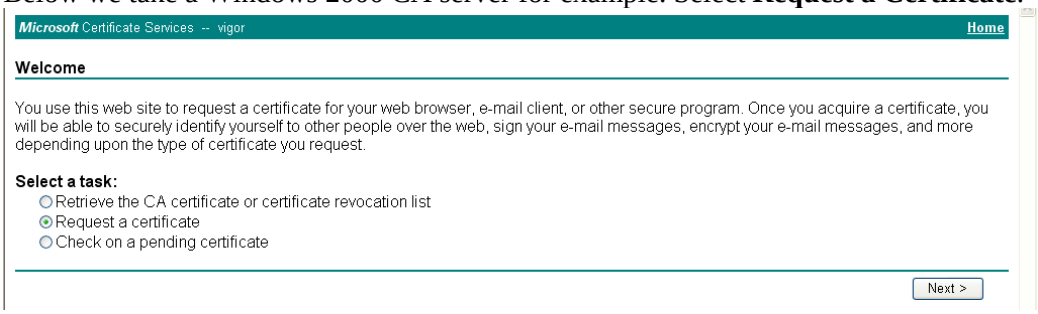
2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.



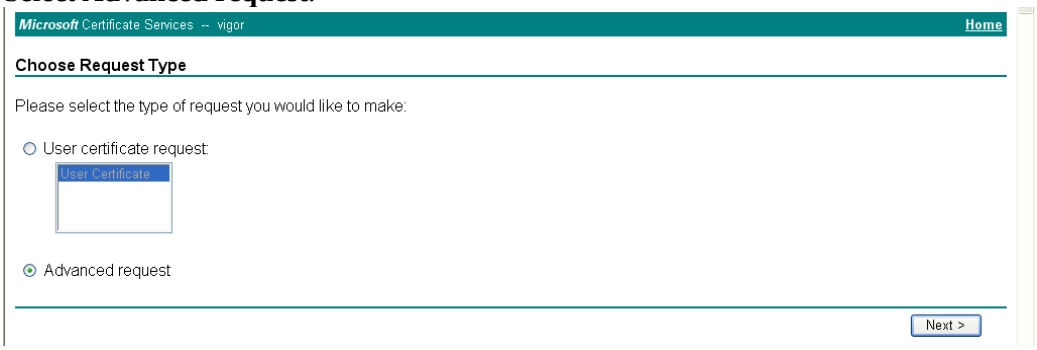
3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use.



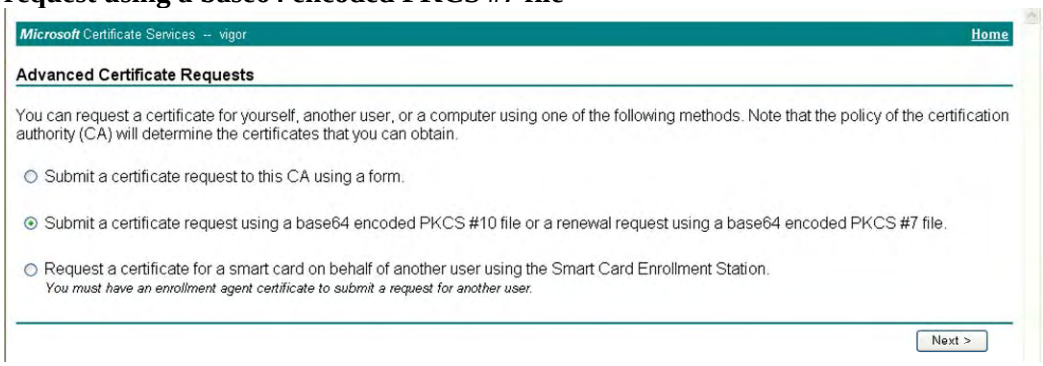
4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.


Microsoft Certificate Services -- vigor
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >

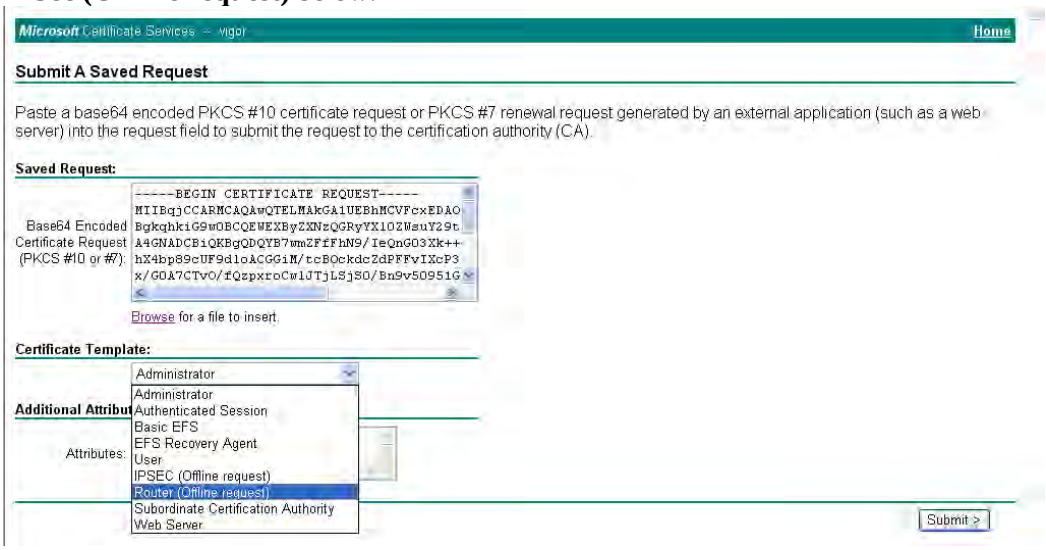
Select **Advanced request**.



Select **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**



Import the X509 Local Certificate Request text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.



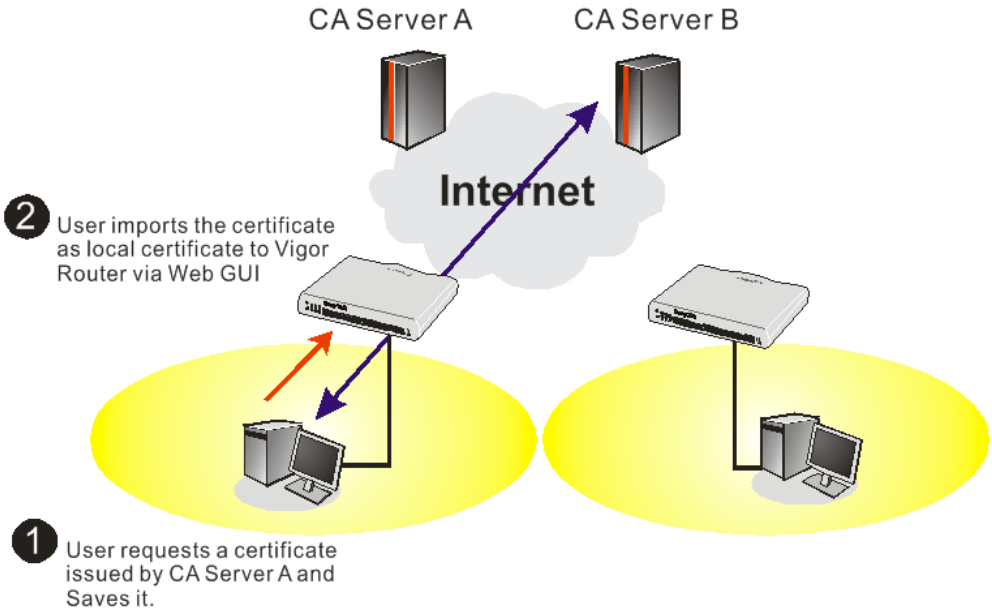
Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and

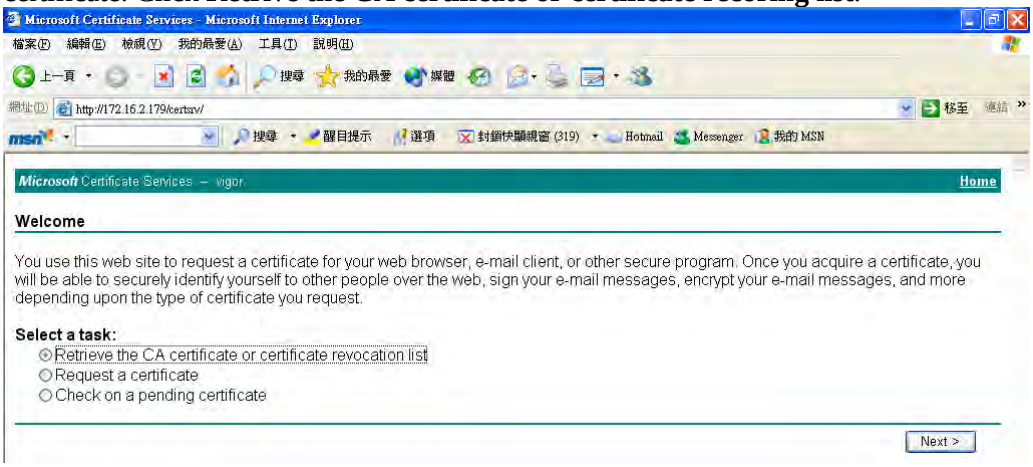
you will find the below window showing "------BEGINE CERTIFICATE------....."

6. You may review the detail information of the certificate by clicking **View** button.

4.8 Request a CA Certificate and Set as Trusted on Windows CA Server


CA Server A
CA Server B
Internet
2
User imports the certificate as local certificate to Vigor Router via Web GUI
1
User requests a certificate issued by CA Server A and Saves it.

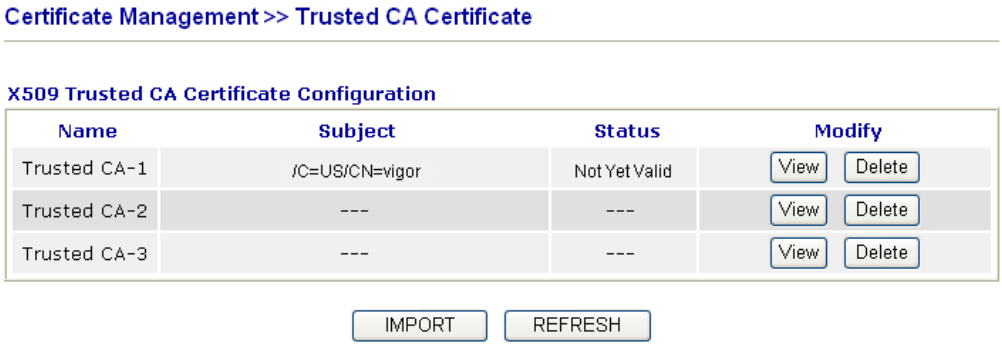
1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.


Microsoft Certificate Services - Microsoft Internet Explorer
http://172.16.2.179/certsrv/
Microsoft Certificate Services -- vigor
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >

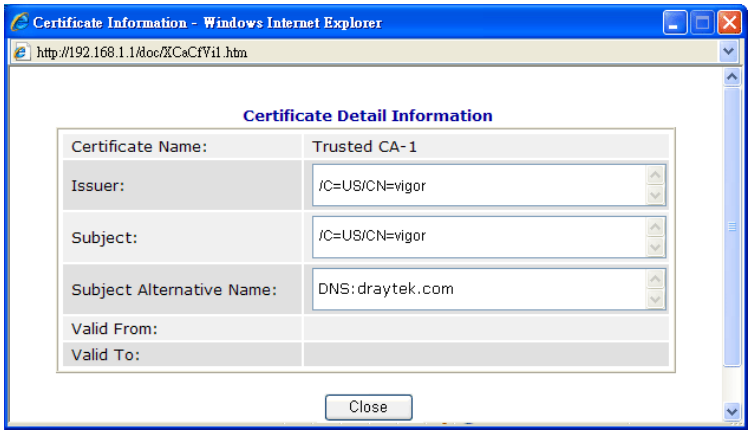
2. In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded,** and **Download CA certificate** to save the .cer. file.

Microsoft Certificate Services - Microsoft Internet Explorer
http://172.16.2.179/certsrv/certcarc.asp
Microsoft Certificate Services -- vigor
Home
Retrieve The CA Certificate Or Certificate Revocation List
Install this CA certification path to allow your computer to trust certificates issued from this certification authority.
It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.
Choose file to download:
CA Certificate:
Current [vigor(1)]
Previous [vigor]
DER encoded or Base 64 encoded
Download CA certificate
Download CA certification path
Download latest certificate revocation list

3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.



4. You may review the detail information of the certificate by clicking **View** button.



Note: Before setting certificate configuration, please go to **System Maintenance >> Time and Date** to reset current time of the router first.

5 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

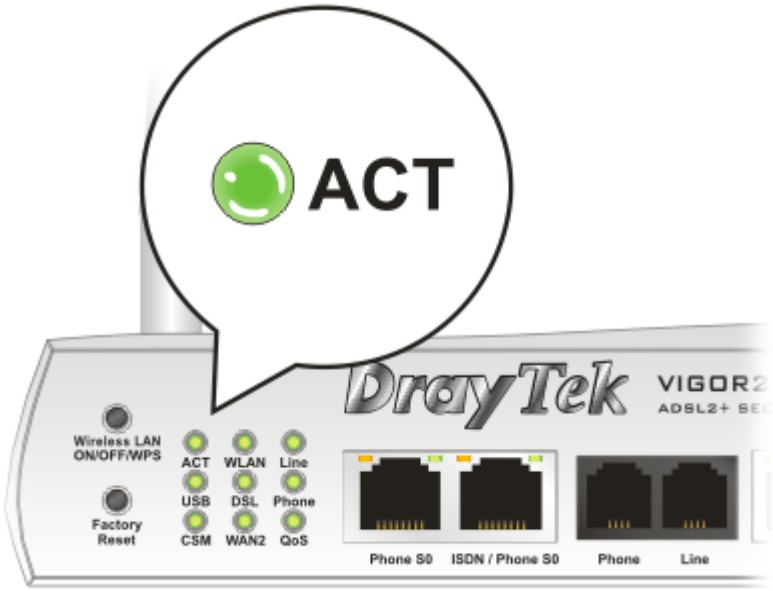
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to "**1.3 Hardware Installation"** for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

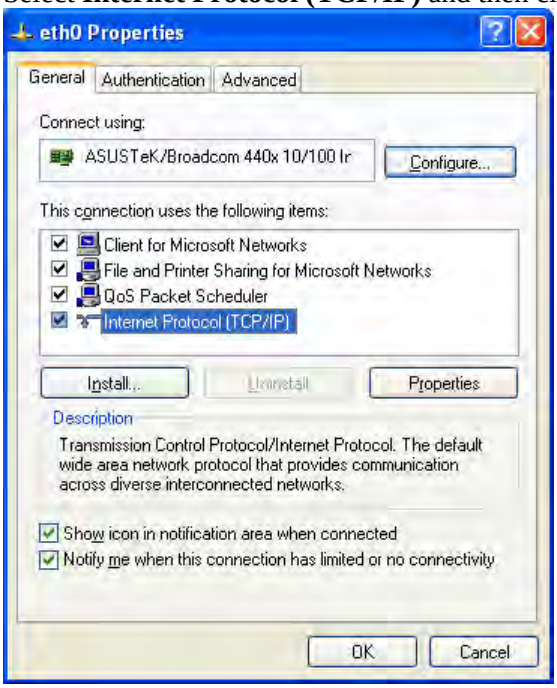
For Windows

> The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Go to **Control Panel** and then double-click on **Network Connections**.

2. Right-click on **Local Area Connection** and click on **Properties**.

3. Select **Internet Protocol (TCP/IP)** and then click **Properties**.

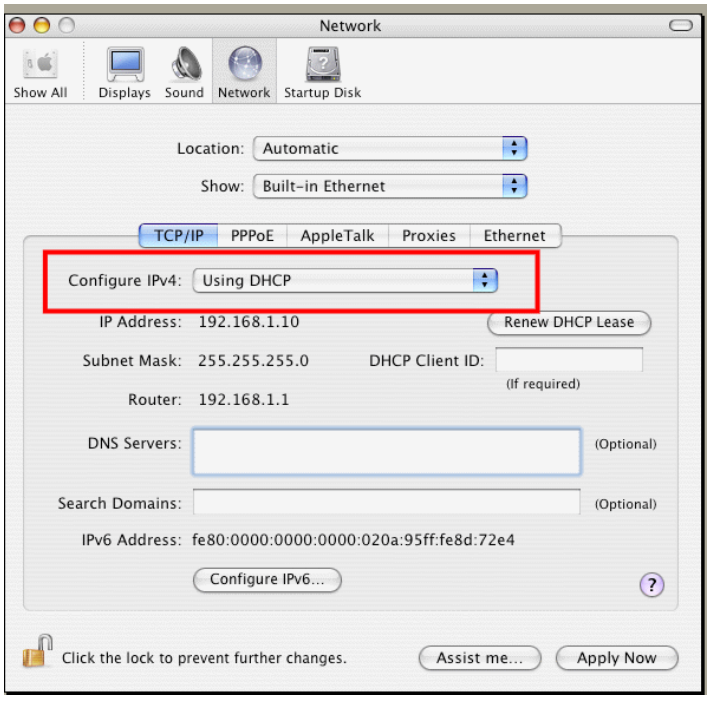


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

For MacOs

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



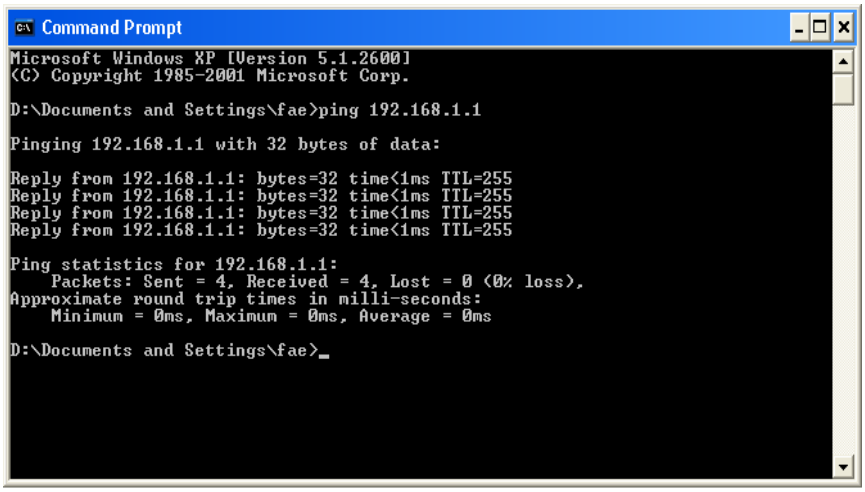
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 4.2)

Please follow the steps below to ping the router correctly.

For Windows

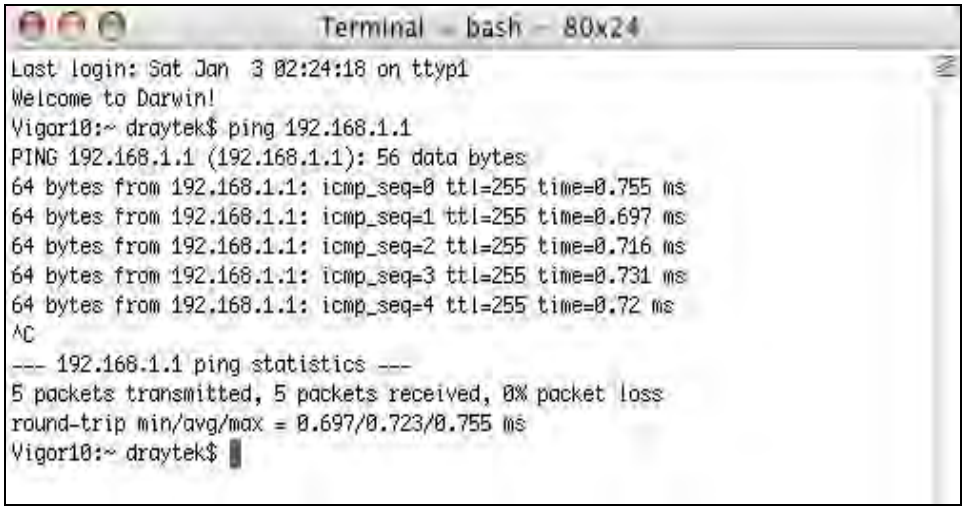
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.


Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
D:\Documents and Settings\fae>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
D:\Documents and Settings\fae>

3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

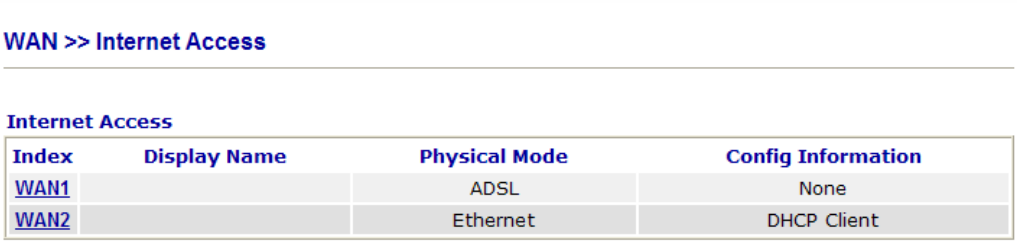
For MacOs (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.


Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

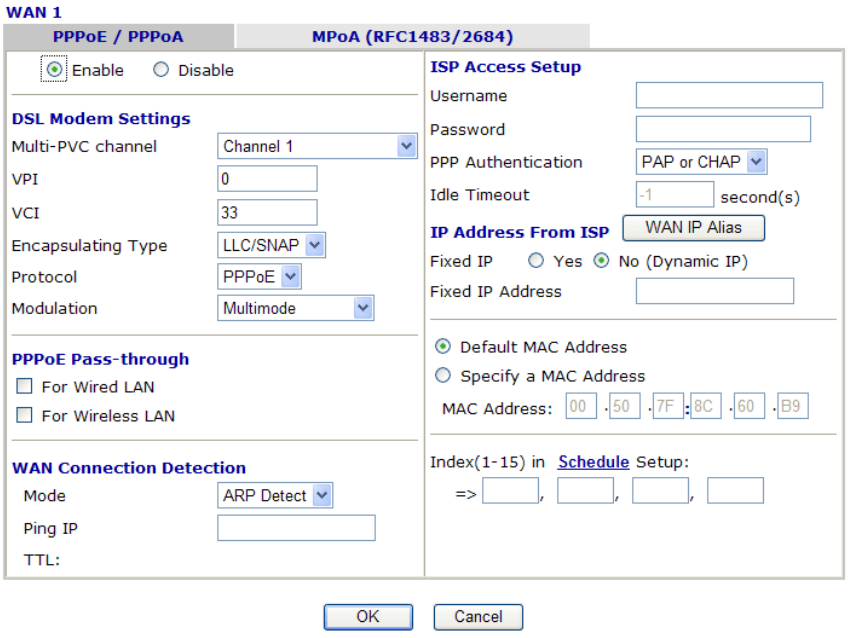
5.4 Checking If the ISP Settings are OK or Not

Click **WAN>> Internet Access** and then check whether the ISP settings are set correctly. Click WAN1 or WAN2 link to review the settings that you configured previously.



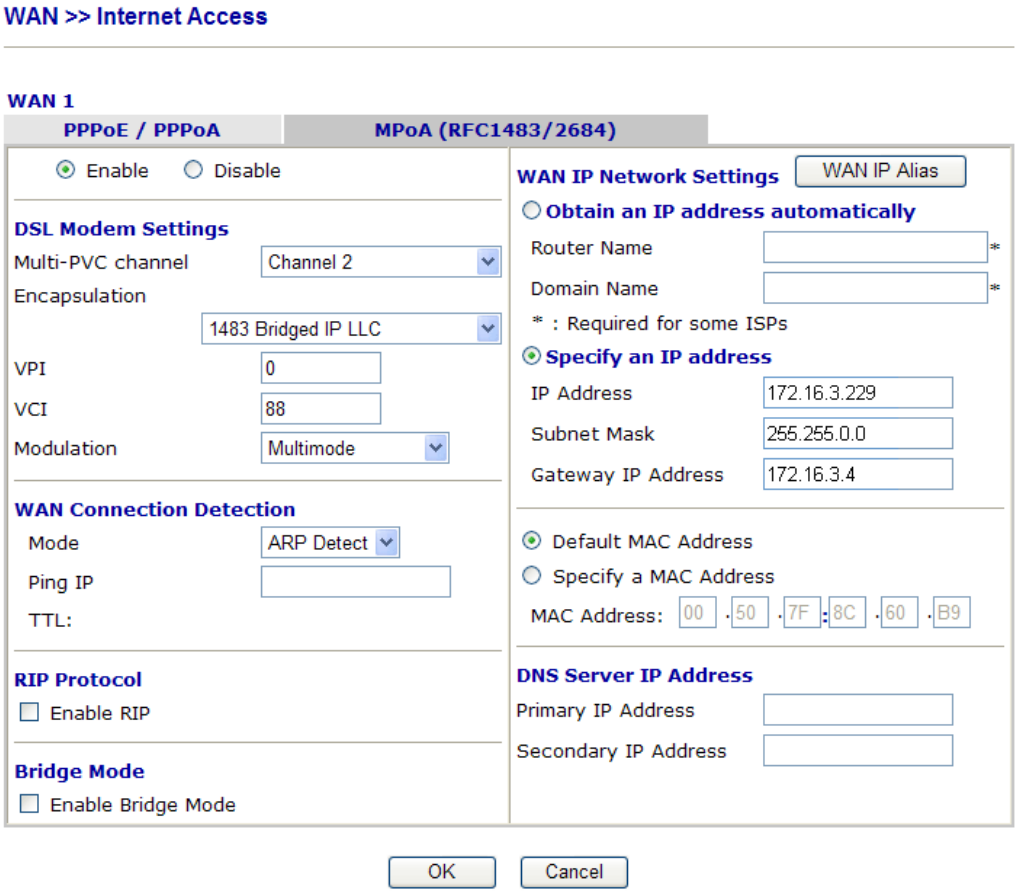
For PPPoE Users

1. Check if the **Enable** option is selected.
2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.



For MPoA Users

1. Check if the **Enable** option is selected.

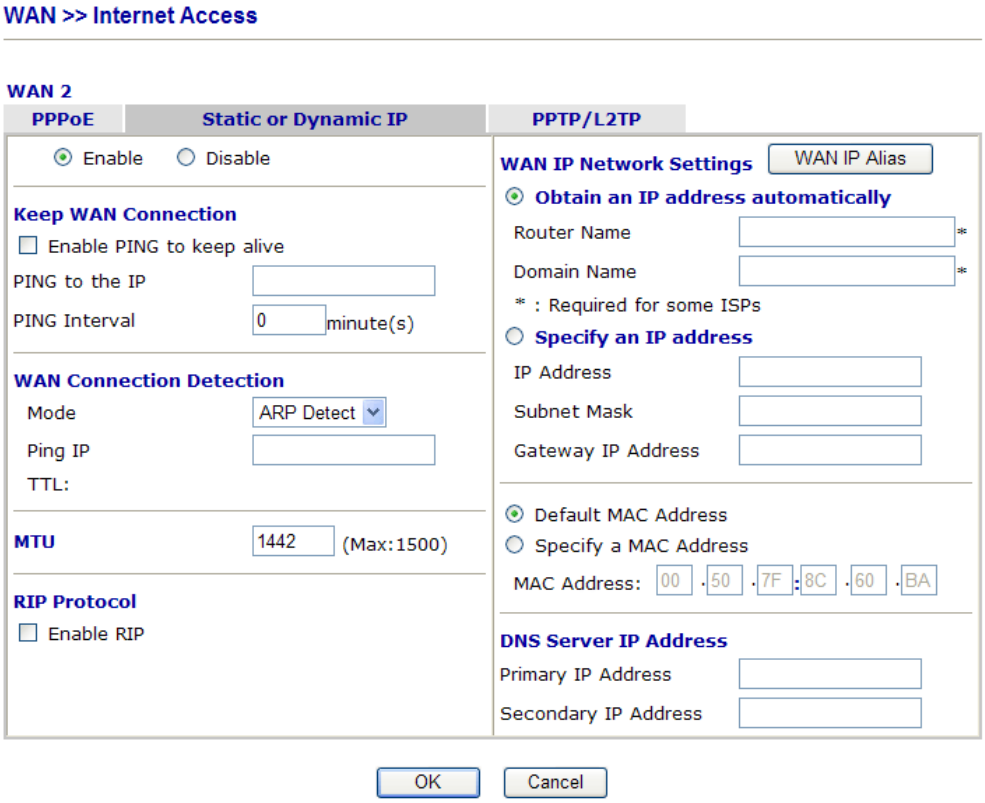


2. Check if **DSL Modem Settings** is set appropriately.

   Check if **IP Address, Subnet Mask** and **Gateway** are set correctly (must identify with the values from your ISP) if you choose **Specify an IP address**.

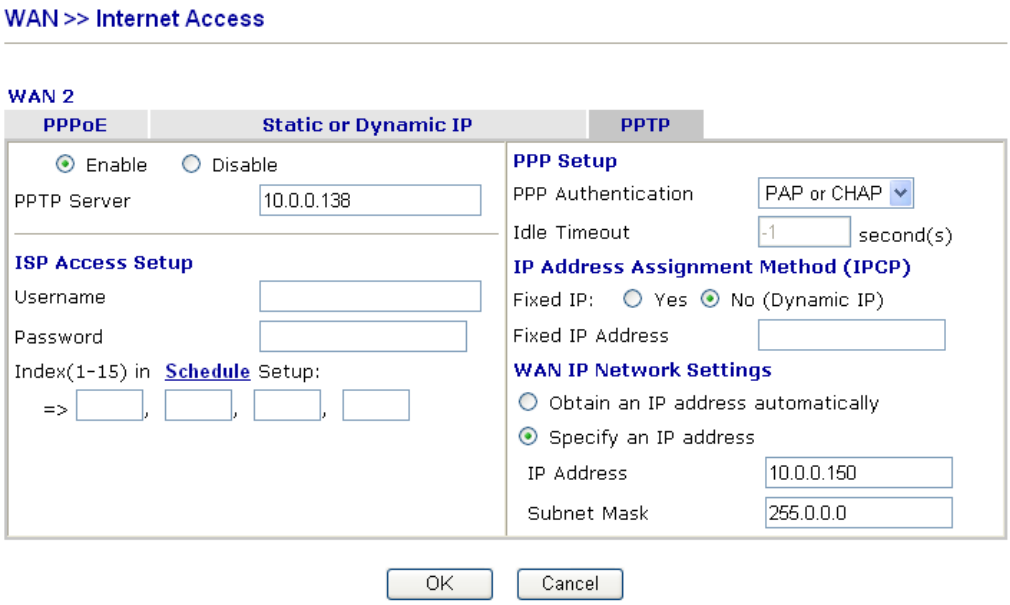
For Static/Dynamic IP Users

1. Check if the **Enable** option is selected.
2. Check if **IP address, Subnet Mask** and **Gateway** are entered with correct values that you **got from** your **ISP**.



For PPTP Users

1. Check if the **Enable** option for **PPTP** Link is selected.



2. Check if **PPTP Server, Username, Password** and **WAN IP address** are set correctly (must identify with the values from your ISP).

5.5 Problems for 3G Network Connection

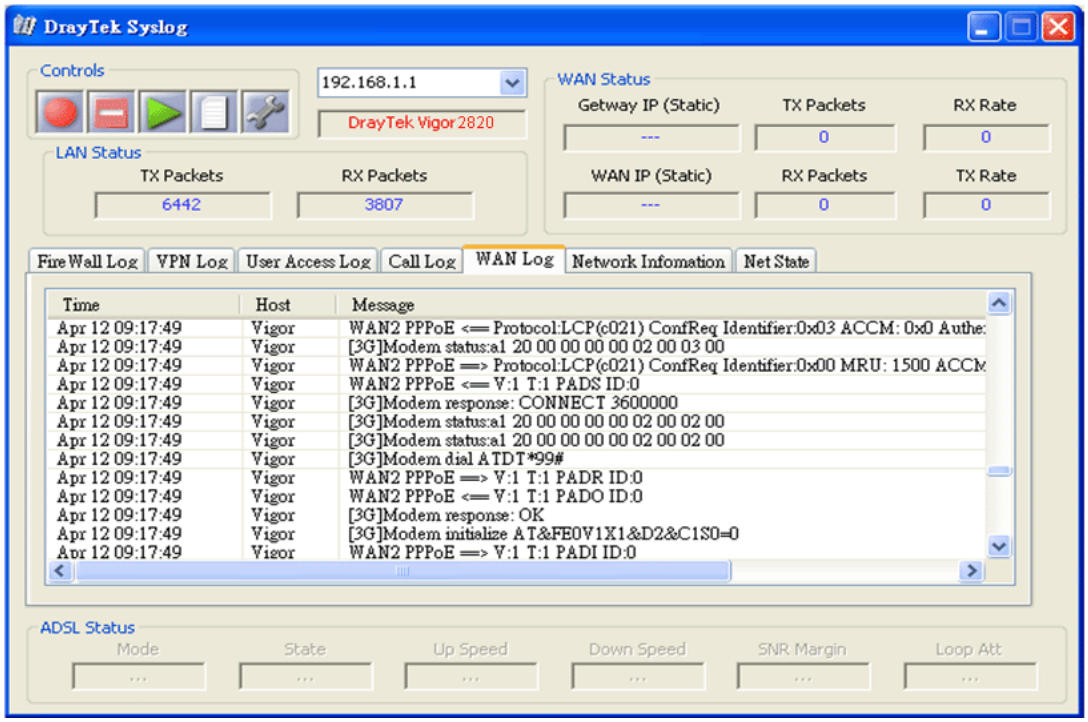
When you have trouble in using 3G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor2820. Later, the USB LED will light on which means the installation of USB Modem is successful. If the USB LED does not light on, please remove and reinsert the modem again. If it still fails, restart Vigor2820.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by Vigor2820. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

5.6 Backing to Factory Default Setting If Necessary

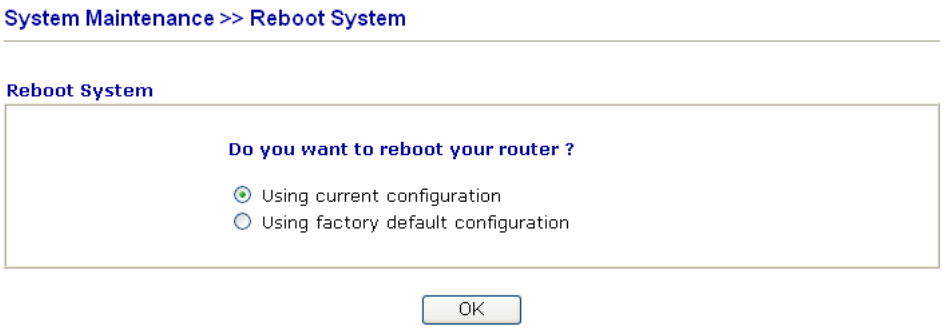
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

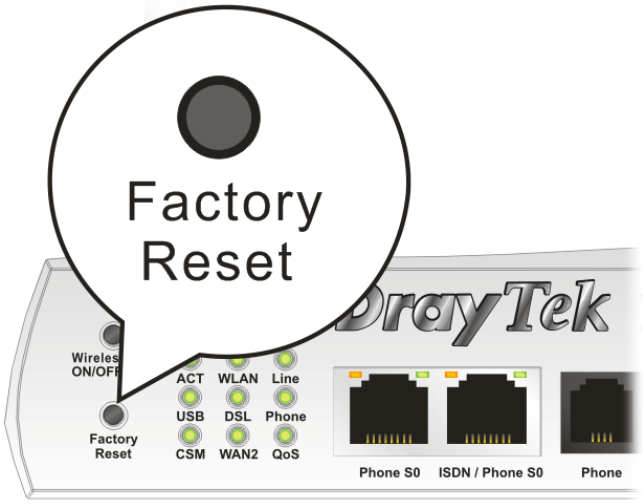
You can reset the router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the router will return all the settings to the factory settings.



Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

5.7 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.

This page is left blank.

Appendix: Hardware Specifications

Temperature	Operating : 0°C ~ 45°C
	Storage : -25°C ~ 70°C
Humidity	10% ~ 90% (non-condensing)
Max. Power Consumption	10 Watt
Dimension	L241 * W165 * H44
Power	DC 12V ~ 15V